Extreme Privacy

What It Takes to Disappear

Second Edition

Extreme Privacy

What It Takes to Disappear

Second Edition

Michael Bazzell

Extreme Privacy:
What It Takes to Disappear
Second Edition

Copyright © 2020 by Michael Bazzell

Project Editors: Y. Varallo, Ashley Martin, M.S. Williams

All rights reserved. No part of this book may be reproduced in any form or by any electronic or mechanical means, including information storage and retrieval systems, without permission in writing from the author. The content of this book cannot be distributed digitally, in any form, or offered as an electronic download, without permission in writing from the author. It is only offered as a printed book in order to avoid invasive digital tracking.

First Published: June 2020

The information in this book is distributed on an "As Is" basis, without warranty. The author has taken great care in preparation of this book, but assumes no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of the use of the information or programs contained herein.

Rather than use a trademark symbol with every occurrence of a trademarked name, this book uses the names only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

Due to the use of quotation marks to identify specific text to be used as search queries and data entry, the author has chosen to display the British rule of punctuation outside of quotes. This ensures that the quoted content is accurate for replication. To maintain consistency, this format is continued throughout the entire book.

The technology referenced in this book was edited and verified by a professional team for accuracy. Exact tutorials in reference to websites, software, and hardware configurations change rapidly. All tutorials in this book were confirmed accurate as of May 1, 2020. Readers may find slight discrepancies within the methods as technology changes.

Introduction 1

CHAPTER 1: Ghost Addresses 11
PO Box / CMRA 11
Personal Mailbox (PMB) 12
Anonymous Mail Forwarding 13

CHAPTER 2: Private Mobile Devices 17
Cellular Telephones 19
Secure Messaging 24
Virtual Private Networks (Mobile) 26
Device Backup and Restoration 28
Secondary Devices 29
Faraday Bag Selection and Testing 31
Telephone Usage 32
Number Porting 34
Number Forwarding 37
Camera and Microphone Blocking 41
Mobile Device Firewall 44
Pagers 45

CHAPTER 3: Private Digital Life 47
New Hardware (Apple) 49
New Hardware (Windows) 56
New Hardware (Linux) 60
Password Managers 64
Two Factor Authentication 69
Encrypted Storage and Backup 71
Browser Configuration 74
DNS Configuration 82
Virtual Private Networks (Desktop) 83
Email Usage 86
Email Forwarding 87
Encrypted Calendar and Contacts 95
Content Archiving 97
Traveling with Devices 98
Tor Browser 103

CHAPTER 4: Nomad Residency 105
Nomad Definition 105

South Dakota Domicile 107
Texas Domicile 108
DMV 109
Residency Affidavits 110
Residency Renewal 114

CHAPTER 5: Legal Infrastructure 119
Trust Definitions 119
Living Trust - Declaration of Trust 121
Trust - Declaration of Trust 129
Appointment of New Trustee 135
Trust Amendments 136
Certification of Trust 138
Choosing a Trustee 141
Limited Liability Companies (New Mexico) 143
Articles of Organizations 146
Certification of Organization 147
Operating Agreement 148
Limited Liability Companies (South Dakota) 159

CHAPTER 6: Private Vehicles 163
Re-titling to a Trust 164
Re-titling as a Nomad 165
New Vehicle Through a Trust 175
New Vehicle as a Nomad 179
New Vehicle Through an LLC 180
New Vehicle Through an LLC as a Nomad 181
Insurance 191
Vehicle Choices 192
Vehicle Privacy 197
Vehicle Tracking 199

CHAPTER 7: Private Temporary Housing 205
Hotels 206
Places to Avoid 213
Rental Homes 214
Hidden Cameras and Unauthorized Entry 216

CHAPTER 8: Private Home Purchase 221
Home Considerations 222
Alias Information 225

Title Companies and Trusts 227
Home Purchase Timeline 233
Home Purchase Issues 235
Neighbors 237
Private License Plate Readers 239
Nomad Home Ownership 242

CHAPTER 9: Anonymous Utilities, Services, & Payments 245
Prepaid Cards 247
Privacy.com 250
Checking Accounts 254
Secondary Credit Cards 255
Secured Credit Cards 260
Alias Wallets 261
ID Scanning and Copying 262
Home Insurance 264
Utilities 269
Amazon 276
Moving Services 278
Appliance Purchases 280
Medical Services 283
Anonymous Purchase Complications 285
Post-Purchase Considerations 287
Virtual Currencies 289

CHAPTER 10: Private Home Network 295
Virtual Private Networks 295
Hardware 296
pfSense Installation 298
pfSense Configuration 299
VPN Configuration 301
VPN Kill Switch 308
DNS Servers 309
Custom Configuration Scripts 313
pfBlockerNG 314
Secondary VPN 317
Wireless/Portable Routers 245

CHAPTER 11: Private Employment 333
Traditional Employment 334
Self-Employment 340

Nomad Business Registration 341
IRS Registration 343
Financial Accounts 344
Contractor Considerations 345

CHAPTER 12: Anonymous Pets 349
Pet Acquisition 349
Pet Services 353

CHAPTER 13: Beyond Extreme 359
Name Change 360
Marriage Considerations 362
Birth Considerations 364
Death Considerations 366
Dual Citizenship / Dual Residency 374

CHAPTER 14: Damage Control 387
IoT Concerns 387
Kindle and E-Readers 390
DNA Kits 392
Fitness Trackers 393
Financial Data Aggregators 394
Family Vulnerabilities 395
Name Disinformation 397
Address Disinformation 399
Telephone Disinformation 404
Business Disinformation 406
Death Disinformation 408
Monitoring 410
Personal Data Removal 413
Consumer Reports 435
California Consumer Privacy Act 438
Online Content Removal 441
Proactive Online Content 452
Credit Freeze and Fraud Alerts 454
Mobile Device Tracking 463
Working from Home 465
Schooling from Home 465

CHAPTER 15: Physical Privacy & Security 467
Home Privacy 467
Home Security 469
Firearms 475

CHAPTER 16: Advanced Private Digital Life 477
Virtual Machines 478
Live USB Operating Systems 487
Advanced Hardware 2FA 489
DIY VOIP 495
Alternative Android Operating Systems 505
RSS Feeds 514

CHAPTER 17: My Successes and Failures: Jane Doe 517

CHAPTER 18: My Successes and Failures: Jim Doe 535

CHAPTER 19: My Successes and Failures: Mary Doe 549

CONCLUSION 565

About the Author

Michael Bazzell

Michael Bazzell investigated computer crimes on behalf of the government for over 20 years. During the majority of that time, he was assigned to the FBI's Cyber Crimes Task Force where he focused on various online investigations and open source intelligence (OSINT) collection. As an investigator and sworn federal officer through the U.S. Marshals Service, he was involved in numerous major criminal investigations including online child solicitation, child abduction, kidnapping, cold-case homicide, terrorist threats, and advanced computer intrusions. He has trained thousands of individuals in the use of his investigative techniques and privacy control strategies.

After leaving government work, he served as the technical advisor for the first season of the television hacker drama *Mr. Robot*. His books *Open Source Intelligence Techniques* and *Extreme Privacy* are used by several government agencies as mandatory training manuals for intelligence gathering and privacy hardening. He now hosts the weekly *Privacy, Security, and OSINT Show*, and assists individual clients in achieving ultimate privacy, both proactively and as a response to an undesired situation.

2ND EDITION PREFACE

The first edition of this book was written in 2018. After an exhausting legal review, it was delayed due to concerns from attorneys. It was finally authorized for release in 2019 and was quickly published after a brief update of the content. Almost immediately after publication, I began working on this second edition. There were many topics I wanted to include in the initial release, but they exceeded the scope of the first edition at the time. Since then, my other books related to privacy have all become out of print. Much of that content was outdated and was overdue to disappear. However, this presented an opportunity to update and combine all of my current works into a single collection. That is what I present here.

I only release a new edition of a book once I have met specific conditions. At least one-third of the book must be brand new content and the remaining material must still be relevant and current. This book contains an additional 200 pages of new content since the original release. Most of the previous writing was still applicable and only needed minor updates to reflect changes since 2018. If you have read the previous edition, you will find most of that original content within this book. However, I have restructured much of it in order to facilitate many new privacy strategies which complement the original text. Throughout the following 560 pages, I have added over fifty unique topics which present many new extreme privacy strategies. I have also included new chapters focused on physical privacy, advanced digital security, and additional client stories presenting new successes and failures as I try to make people disappear. To me, this feels like a whole new book.

I also dropped "In America" from the subtitle of the original book. I heard complaints from many international readers who believed including a specific country in the title was off-putting. I agreed and removed it for this and other reasons. Most of the new content in this second edition is globally applicable. Over half of the book now applies to the entire world. I believe the remaining half, which focuses on my experiences in the U.S., can benefit everyone. My hope is that readers apply my strategies, which include LLCs, trusts, nomad registration, employment, anonymous purchases, and other U.S.-focused tactics, toward the opportunities available in their own countries. While this book will benefit residents of the U.S. more than anywhere else, the lessons should be digested by non-Americans for replication outside of my country. I can never present options for every location, and only include my own experiences. However, I hear from many international readers about numerous successes on their own turf.

My goal is to maintain this book with updates when at least one-third of it contains new information. Considering how quickly technology changes, and new threats toward our privacy emerge, this should unfortunately be an easy task.

I am excited to now introduce yet a new level of extreme privacy. ~MB

Introduction

Extreme Privacy

Maslow's hierarchy of needs prioritizes our most fundamental requirements as basic physiological demands, physical safety, and then social belonging. Many have simplified this as food, shelter, and love. Most of my clients adapt this to anonymous purchasing options, a ghost address, and a clean alias.

I should probably back up a bit here and explain some things about my career. I spent over twenty years in government service. After eighteen years in law enforcement as an investigator for various agencies, I spent four years focused on extreme privacy strategies as a major part of my privately-held company and as a contractor in the intelligence community. During the majority of my career, I was a sworn task force officer with the FBI, where I focused on cyber-crime cases and creating a software application for automated Open Source Intelligence (OSINT) gathering. My time with the FBI made me realize how exposed we all were, and that privacy was dying.

In 2002, I developed a strong interest in privacy and eventually wrote a book titled *Hiding from the Internet* which helped people clean up their online lives and become more difficult to find. After working covertly with criminal hackers, I was concerned about a growing phenomenon called "doxing" which happened to many of my coworkers. Doxing is the act of publishing complete personal details about a person online. This usually includes full name, home address, telephone numbers, family members, date of birth, social security number, and employment details. Others can then use this information to wreak havoc on the person with prank calls, delivered packages, and occasionally personal visits. I did not want to ever be on the receiving end of this, so I took action to remove all publicly available details about me from the internet. I never expected it to become my occupation.

I began teaching large crowds about these techniques which went as far as completely disappearing from any public records and becoming "invisible". I was determined to perfect the art of personal privacy. My focus changed from removal of public information to intentional disinformation which caused confusion to anyone trying to stalk someone whom I was protecting. Eventually, I developed complete solutions to starting over with a new life that could not be connected to the previous. Often intense and extreme, my ideas were not always accepted by every potential client.

I eventually left government work as I wanted to commit to a completely private life and continue to help others disappear. I was extremely fortunate to be asked to help write the first season of a new television drama called *Mr. Robot*. The idea was to make all of the hacking and technology realistic, which I believe we accomplished. The show received high accolades, including a Golden Globe award for best drama, which introduced many new opportunities for me with the press and online media. This led to additional conversations with A-List celebrities, producers, and other Hollywood moguls. When combined with my ten years of public speaking side-gigs to financial companies and other large corporations, I immediately had access to a huge audience of wealthy people with problems. Once my services were known within this circle, word-of-mouth kept me busier than I could have ever imagined. From nude photos being released on the internet to attempted abductions, I became known as the guy who "fixed" things.

Today, my primary focus is on extreme privacy and completely disappearing from public records. Every week, someone contacts me with an urgent need to fall off radar. Something bad has usually happened, and there is a concern of physical safety. This is where my extreme antics are welcomed, and I execute a plan to make my client invisible to anyone searching for him or her.

I will never share the exact details applied to my own privacy strategy, but I have executed numerous examples throughout this book toward my own life before attempting on others. I always try to fail at a new technique while practicing against my own personal information before attempting with any client. Sometimes, there is not time for this luxury, and I must pull the trigger on the fly and hope for the best. I have definitely made my share of mistakes and I have numerous regrets when it comes to the techniques used to achieve this lifestyle. You will read about many of them here. There was no textbook for this and I had no one to consult with before trying to officially disappear on my own.

Many clients do not need to erase their entire lives. Some just need help with a specific situation. Lately, the majority of people who contact me have had something negative posted about them to the internet and they want it removed. This can be very difficult as most search engines ignore these types of removal requests. Some people I cannot help. A recent client was arrested and his mugshot was plastered across numerous websites. I cannot always erase those, but I disclose my methods later in this book. A surprisingly high number of women contact me after a former lover posts pornographic videos to adult websites in attempt to shame them for leaving. These are fairly easy to remove when enough time exists to scour every source. Some clients present tricky situations such as defamatory comments on blogs and personal websites. These require a delicate touch, and most can be removed.

My most difficult clients are those whom I never meet. Occasionally, a very wealthy or extremely famous person will need my services. Most of these individuals meet directly with

me and we start their privacy journey. However, some are too big to meet with me face-to-face. Instead, I meet with teams of lawyers which are skeptical of my methods. They then communicate with an assistant to the actual client who then later speaks directly to the client. Much is lost in translation, and I am asked to clarify my strategy. This generates a lot of confusion and misunderstandings. Worse, the execution of my plan is done incorrectly and therefore is not successful. After a few meetings, I am dismissed and I never hear anything from them again.

On one occasion, a famous movie actor reached out about the purchase of a new home and did not want to have his name associated with the paperwork. He wanted it to be a retreat off the radar of the tabloids. I was only allowed to meet with his personal assistant. She seemed very competent at orchestrating his life, but knew nothing about privacy. She unintentionally misspoke to the real estate attorney, which I was not allowed to meet, and the closing paperwork included a single mention of the celebrity's name. Within weeks, an aerial photo of the estate was in a tabloid identifying the new owner.

There are many clients with which I decline my services. After a few years of providing privacy consultation as a "hidden" service, news spread of the successes achieved with a handful of well-known clients. This resulted in a huge increase of strangers contacting me through my website about their own situations. Many were very honest about their true identities and even more candid about the scenarios with which they were seeking help. Others were very vague about everything and became concerned about me knowing too much about their situations.

One of these was an individual that went by the name "Nobody" through a throwaway email address. He asked if I could help him disappear to the point that no one in the United States could find him. He had a large amount of cash that he wanted to use to buy a house anonymously. He refused to provide his real name which is an absolute deal breaker. If I can't vet a potential client through various verification procedures, I am not interested in helping. I had considered immediately declining his request, but I was too curious about him. Was he Tom Hanks? Does he operate a hedge fund? How did he get all the cash and what was he running from? I played along for a while and convinced him that he should install a secure communications application called Signal on his mobile device. Signal allows users to communicate securely with other Signal users by providing full end-to-end encryption for all voice, video, and text communications. This prevents anyone from intercepting the connection and even Signal employees cannot identify the content of the communication.

I was not interested in talking to him through Signal, but I was counting on him making a common mistake when he installed the application. Signal uses your cellular telephone number by default when you install the service. You then give the number to other Signal contacts and begin talking securely. I did not ask him for his Signal number, because he would likely feel exposed by disclosing his actual cellular number, even if only used through Signal. Instead, I

gave him my Signal number and told him to send me a verification text within the Signal application. My Signal number was a Google Voice number that I dedicated solely for use on Signal. This way, no one could connect my Signal account with my real cellular account. The potential client sent the text, which arrived in my Signal application. It immediately revealed his true cellular number.

I provided this number to various telephone search services to which I subscribe and collected the results. Within less than a minute, I possessed a true name, home address, email address, and Facebook page associated with his cellular number. It belonged to the girlfriend of a fugitive wanted by the U.S. Marshals for many serious crimes including molestation of children. This is the reason I vet everyone. If I were to assist a federal fugitive, I could be prosecuted myself.

My gut said to simply stop communicating and walk away. I couldn't. I knew from the beginning that this was suspicious. The need to pay in cash and the desire to only disappear from anyone looking for him in the U.S. were red flags. After some brief conversation, I was positive he was the wanted pedophile fugitive. I told him that I could meet him in Los Angeles in a week. He should bring $5,000 cash for my retainer and have it in a Taco Bell paper sack. His girlfriend's previous home address was only an hour outside the city, so this seemed plausible for him to agree to the meeting. I picked a quiet location that would not have too many people around early in the morning on a Sunday. I told him I would be wearing a blue shirt and black jeans. I would have glasses and a trimmed beard. He volunteered that he would be in a rented BMW and wearing a red collared shirt with tan shorts. I then did something that may offend some readers. I immediately called a U.S. Marshal contact that I had made during a recent internet intelligence training that I had conducted in the Los Angeles area and let him take over.

To this day, I have no idea what happened on that Sunday morning. My guess is that an arrest was made, as that subject is no longer on the public fugitive list. Why the Taco Bell paper sack? It is a great way to identify the suspect in the case that multiple people fit the general description. Please know it is rare that I need to utilize this type of ruse in response to a solicitation by a potential client, but I refuse to have my services exploited by child predators. If it were a misdemeanor warrant for shoplifting food, I would have taken no action and you would not be reading this. However, with certain serious crimes there is a clear moral obligation to intercede. Also, it should be noted that when someone hires me to make them disappear, I need to learn most of their private details if I am going to effectively obfuscate them.

Other declined clients include those that I simply cannot help. Some have mental issues that have created unnecessary paranoia and a constant concern that they are being monitored. They often send me twenty-page emails that contain random thoughts that seem incoherent. I try

to convince those people that they are likely not in any danger and should seek counseling to eliminate some of these stresses. Occasionally I follow-up, but rarely receive a response. Others are simply not ready to go the distance. They want to continue to use Facebook, Twitter, and Instagram while having an expectation of privacy during their new life. I do not believe that any of my clients can truly become invisible and still use social networks. Some of those who stay off the main social networks are still not ready to eliminate their online lives.

On one occasion, I helped a young woman remove revenge pornography from the internet. She had sent very intimate videos taken of herself with her telephone camera to a current lover with whom she would later end the relationship. He posted them online and I used various tactics to force removal. A month later, she sent similar videos to a new lover that posted them online during their relationship, and attempted to extort her after she left him. I removed everything, including cached copies on search engines. I encouraged her to stop trusting others with this sensitive content. Three months later, she asked how she could remove new photos of herself engaged in a recent sexual act from an adult website, posted by her latest ex-boyfriend. I wished her the best, but advised that I had exhausted my ability to keep her private. I encourage those who value their privacy to trust no one with nude photos. The internet will ensure they are conveniently published and stay online forever.

My favorite clients are the people who are ready to start over. Relocation is mandatory and alias names will be used daily throughout the rest of their lives. They will never associate their true name with any purchase or location ever again. They are prepared to embrace the additional effort it will take to properly respond to daily requests for their personal details. A trip to a dentist, chiropractor, barber, hotel, restaurant, or Starbucks will never be the same. They will immediately realize the number of personal details which are collected about them every day, and the impact of divulging accurate information on their personal privacy. This requires a strong desire to disappear and the discipline to maintain the lifestyle. They will be impossible to find if done right. This book is written for that type of person.

My previous books about privacy were mostly REACTIVE. I focused on ways to hide information, clean up an online presence, and sanitize public records to avoid unwanted exposure. This book is PROACTIVE. It is about starting over. It is the guide that I would give to any new client in an extreme situation. It leaves nothing out, and provides explicit details of every step I take to make someone completely disappear. Many readers are likely questioning the reasons someone would need to execute the exhaustive plans that I have created. Almost all of my clients fall into one of four categories.

The Wealthy Executive: This represents the majority of my work. After living a traditional life with their family's name attached to everything they do, something bad happens. Layoffs at the company launch death threats to the CEO or a scandal breaks out indicating that corruption rises all the way to the top. Whatever the situation, my client wants to disappear.

They want a safe place for their family to stay while things get sorted. This is surprisingly difficult. Hotels want valid ID, and social engineering attempts by journalists and enemies quickly identify the location of the client. I will explain many ways that I secretly hide people temporarily and permanently.

The Celebrity: My famous clients usually have one of two problems. They either made a mistake and now need something cleaned up (such as nude photos, inappropriate tweets, or inaccurate articles), or they want to buy a new home that will not surface on tourist maps. I will present many pages within multiple chapters discussing the options for completely anonymous home purchases. It will not be easy, but it is possible.

The Government Employee: At least once a week, I am contacted by a police officer or other government employee that is in immediate danger. He or she is involved in a high-profile shooting, court case, or cartel investigation, and the spotlight is on. People are looking to cause problems and the client finds their home address on hundreds of public websites. It is too late to clean-up. It is time to move, and it is very important to be strategic about the names associated with any lodging.

The Victim: This is usually my most cooperative and eager client. It is also usually a woman. She finds the courage to leave a physically abusive relationship and she knows that her safety depends on her disappearing. I have had clients who were victims of attempted murder who know they must now live an anonymous life. This requires a long-term game plan, and each step of the execution must be perfect. Their life is relying on anonymity.

I am fortunate that I can now pick and choose the clients that truly need the help and will successfully execute the plans that I create. While I rarely meet new clients due to a series of fortunate events, and most come to me to "fix" something, the final result after I finish my work is usually positive. Some of my clients have had devastating events impact their lives, but they have moved on and are now happily invisible. It has not been all roses. I have made many mistakes and learned expensive lessons about my privacy strategies. Some of my less than optimal ideas have landed me in hot water, and even in physical police custody during one unfortunate event (which is not discussed here). I hope these lessons assist others with properly executing their own strategies and not replicating my mistakes.

Some will think that this book will hide them from the U.S. Marshals or prevent them from serving a pending prison sentence. It won't. I know the groups that will be in charge of hunting you. They are good. They will find you. Even fugitives who escape to the woods without any possessions get caught. This is not that type of book. This is for the increasing number of individuals that no longer want their home address on Google; data mining companies to build detailed profiles of them; or health insurance companies to snoop on their private purchases. They are tired of companies "listening" to their devices through metadata and questionable

permissions. They simply want out of the system which allows data within their digital lives to determine how they are treated by large corporations and governments.

When I was a child, there was a single choice you could make which either made you private or public. You could specify that your telephone number be unlisted. This action removed you from the telephone book, for a small fee, and made you practically invisible. This is laughable today. The moment you deed your home in your name, it is public information on the internet. Did you start electricity services at your new rental home in your real name? Within days, data mining companies replicate these details; append your social networks and family members; neatly package your profile into a sellable product; and offer it to any new startup looking to target you with advertisements. It is a mess, and I believe we should take steps to stop this behavior.

The advice within this book is NOT to move to the woods and cease contact with everyone. It is quite the opposite. I believe that you can lead a normal life, including healthy relationships, without making personal details public. There will be a balance of enjoyable living and refusal to submit to the standard abuses of data collection. As I navigate through the book, there will be many times which you can choose the level of adoption. While I will always present the suggested extreme methods, there will be opportunities to slowly slide into privacy. Please read the entire book before executing any strategies of your own.

It is highly unlikely that you will need to completely disappear. Hopefully, you get through life without the requirement to hide. However, I ask you to consider all of the strategies presented here. While they may not all apply to you, there are many steps you can take to better protect your personal privacy and security. The book is written in chronological order of every step that I take with a new client requiring the full treatment. It is presented as if you are in immediate danger of losing your life, and people are trying to find you. It attempts to put you back into a normal life without the need to constantly look over your shoulder. Many of these tactics are extreme. You may laugh out loud a few times. Your family and friends may think you are crazy. However, if you ever need to disappear, you will be prepared.

The information shared in this book is based on real experiences with my actual clients. The following stories are all true, with the exception of changed names, locations, and minor details in order to protect the privacy of those described. Every subject referenced in this book has given both verbal and written consent to appear in the content, and possesses an interest in helping others in similar situations. I have refused to share their true identities with anyone, including my publisher, legal advisors, and other clients. I take my clients' privacy very seriously.

Finally, you will see the following statement a few times throughout this book. It was required by my legal team, but I agree with every word.

I am not an attorney. I am not YOUR attorney. You should not replicate anything I discuss in this book without first consulting an attorney. The following is not legal advice. It is not any type of advice. It is merely explicit examples of the actions I have taken to make myself and my clients more private. Your scenarios will be unique from mine and your privacy plan will require modification from mine. Seek professional legal advice.

Chapter One

Ghost Addresses

Most privacy enthusiasts already have a United States Postal Service (USPS) Post Office (PO) box. This is a great layer of privacy for mailings in a real name that you do not want associated with your home. I have possessed many PO Boxes over the past two decades, but I will never use one again. The requirements for obtaining a PO Box have not changed much, but the residential enforcement has increased substantially.

Postal Service form 1093 is required in order to obtain a PO Box. This form explains that valid government identification must be provided, which seems acceptable in my view. Section four of this form is where I begin to get frustrated. This section requires your current home address, and this information must be verified by a postal worker. The verification is usually made via a delivery person who can confirm the applicant receives mail in that name at the residence. In other words, you must receive mail in your real name at your real address in order to obtain a PO Box to receive mail. If you cannot obtain verification of this, you will not receive your box. This means that a homeless person cannot obtain a PO Box, which seems to be an ideal need for the service.

Over the past year, I have seen enforcement of a confirmed home address at an all-time high. In 2018, I was assisting a client with the purchase of a new home in a city with which she was unfamiliar. She needed a PO Box in order to receive important documents and payments, and had not yet found a home she liked. The hotel where she was staying did not allow daily mail to guests. I entered the local post office and asked for an application to rent a PO Box. The employee immediately asked if I had a local address. I advised I did not and that I was house shopping and will be here a few months while I decide. I was shot down right away and told I could not have a PO Box unless I had a local address. I caved a bit and said that my local address is currently a hotel. No dice. This seems ridiculous, and is becoming a common result when I enter a post office. I have quit trying. Instead, I rely heavily on Commercial Mail Receiving Agencies (CMRA).

A CMRA may be better known as a UPS store or a mom and pop style shipping store that provides mail boxes. These services will usually charge a higher fee than the post office, but the verification requirements are almost always less demanding. Additionally, the service is usually superior and there are less restrictions on deliveries from UPS, FedEx, and other services. You will still need to complete a USPS form within the UPS system, but the address verification is usually waived. You must provide the names of all people who might receive

mail at this box. In my experience, UPS stores are not as strict about this as USPS PO Boxes. I have never had a piece of mail in a random name refused at a UPS store, but this has happened often at the post office. If you obtain a UPS box, I highly recommend adding the name of a generic LLC to the list of potential recipients. LLCs will be explained later. This will give you an option to have packages delivered to your UPS box in the name of the LLC, or variation of it.

In 2018, I opened over a dozen UPS store boxes on behalf of clients. In every situation, the only identification shown of my client was a passport and utility bill. The passport does not possess a home address, and the utility bill displays a former address which will no longer be accurate after a new home is purchased. In every scenario, the address provided was not local to the area. I received no resistance from the staff, and walked out with a new box and key that day.

A UPS box is not a ghost address. It is a very obvious commercial mailing address which will not pass for a true residential address within systems that scrutinize this type of data. While most UPS stores advertise that they provide a residential address, this is mostly marketing. At a post office, they demand that you use "PO Box" within the mailing address, and a UPS store allows you to use your box number as "suite", "unit", or other possibilities. However, this does not fool big brother.

If you try to open a new bank account and provide a PO Box or CMRA box, you will likely be denied. If you try to use the UPS box on your driver's license, expect failure. Practically every CMRA agency address has been identified within a database that is used by most financial, government, and related institutions. The moment you place a CMRA address within a credit card application, it is flagged for review. Therefore, a simple PO Box or UPS box is not sufficient for our needs. We need a true ghost address that appears like a residential location; allows us to receive mail sent to that address; and never requires us to physically be present at the location. We need a PMB.

A Personal Mail Box (PMB) is much more than a simple PO Box address. It provides you a true residential mailing address, which is often accepted by institutions that otherwise block CMRA and PO Box addresses. It also allows the collection of mail and distribution to a second address of your choosing. It is basically your new permanent personal address for any mail delivered in your real name. A PMB is a staple for every client. It is also a vital step toward advanced privacy techniques such as obtaining proper vehicle registrations, driver's licenses, passports, and other identification documents. All of this will be explained in upcoming chapters.

Most states have companies which will provide a PMB, but I only recommend South Dakota and Texas. I had previously considered Florida as a candidate for PMBs, but I no longer

endorse this option. Obtaining a PMB is a small part of a larger privacy strategy which will be explained later, and I have had complications including Florida within that strategy. Therefore, I will focus on the only two states where I have continued success.

South Dakota and Texas are very friendly to full-time travelers such as those who live in an RV or nomadic people who explore the world year-round. This has spawned a business opportunity for companies wishing to cash in on the needs of these travelers, such as mail service. This chapter will only discuss your mailing needs, while future pages will explain how you can take this to the next level. I encourage you to finish the entire book before committing to a specific state or provider.

I do not have much preference of one state over the other for PMB services. Most clients choose the state that makes the most sense for them geographically. Clients in the northwest and near the Rockies tend to use South Dakota while clients in the south or east choose Texas. Regardless of the state, I highly recommend PMB services by a company called Escapees. Escapees is a Texas business, but they have a satellite option in South Dakota as well. Please note that I am NOT a sales affiliate of Escapees and that I have no financial interest in the company. I have tested many PMB services, and Escapees has been the most appropriate for the needs of my clients. Many of the PMB services I have tested possess awful security protocols, and Escapees has been the lesser of all evils when it comes to digital protection of their assets. The following will walk you through the steps I take on behalf of a client to establish a new residential PMB.

First, download the Escapees Mail Service Agreement for the state of your choice from their website at escapees.com. The default service is in Texas, but they recently added a South Dakota option. At the time of this writing, the forms were at the following addresses.

South Dakota:
escapees.com/wp-content/uploads/2018/08/303w_mail_service_agreement_sd_1017.pdf

Texas:
escapees.com/wp-content/uploads/2018/08/303w_mail_service_agreement_tx_1017.pdf

I encourage my clients to choose the lowest tier (Category A) of service plus the mail scanning feature. This allows Escapees to provide you with a unique PMB address which can collect and store any incoming mail, and be shipped to you practically any way desired. You can schedule mailings of all collected mail to any address, such as a UPS box or hotel. The scanning feature provides an email with a digital scan of the envelope of all incoming mail. This allows you to be informed when anything important arrives which you want forwarded. Be sure to select the option to allow Escapees to sign for packages on your behalf. Part of this application

is U.S. Postal Form 1583, which allows Escapees to accept and forward your mail. Most of this is self-explanatory, but I want to highlight a few important areas.

Box 2 must include any names which may receive mail. This is not the time to be vague. You should include nicknames and maiden names. You should also include the names of at least one trust. Later, I will explain how to use trusts as a layer of privacy within ownership of assets. If you have no trusts listed, mail sent to those trusts might be returned. In my experience, if you have at least one trust title listed here, even if it has not been established yet and is different than the trust name you will later use, it increases the likelihood that you will receive mail addressed to any trust at that PMB.

Box 8 requires a current home address. This can be any mailing address that you currently possess, and I have never witnessed any verification process. Since I assume that you will be moving in the near future in order to obtain true privacy, this can be your current home address.

The instructions for Box 9 indicate that you must be a current Escapees member. This is not actually true. You must first submit a copy of at least one government photo ID. I encourage you to submit a copy of your passport or passport card, as these do not contain a home address on them. The second required ID does not need a photo, but must have some type of unique number that can be tracked to you. This can include a military ID, Driver's License, or AARP card. For most clients, I submit the driver's license, especially if he or she will be moving soon to a new address.

The form must be signed in front of a notary. The application will be rejected without this. Once the form is complete, and you have included some form of payment, it takes about a week to receive your welcome packet including your new PMB address and number. Note that a credit card is accepted on the form, but please use a masking service as discussed later. Your new address will appear as one (or both) of the following.

316 Villa Dr. #143
Box Elder, SD 57719

101 Rainbow Dr.#143
Livingston, TX 77399

One benefit to using the Escapees South Dakota option is that you actually receive two mailing addresses. The South Dakota address can be used later for a driver's license and vehicle registration while the Texas address can be used as a traditional PMB. This comes at a cost. Every piece of mail that must be forwarded from South Dakota to Texas, before being forwarded to you, extracts $1.00 from your postage balance. If you plan to eventually obtain a South Dakota driver's license, vehicle registration, or business license, you should choose the South Dakota option. If not, choose Texas. If you plan to eventually obtain a Texas driver's license, vehicle registration, or business license, you should choose the Texas option.

If you like the idea of having two ghost addresses in two separate states for the same price as one, South Dakota is for you.

You can now begin changing your mailing address for anything important to you. This includes your banks, brokerage firms, credit cards, and anything else that does not care that you reside in a new state. At this point, you are not a resident of South Dakota or Texas, you simply possess a mail forwarding service. As you update your mailing address with various institutions, they will begin to report this change to the major credit bureaus and data mining companies. Consider filing an Official USPS Change of Address form at your local office. Choose the "Permanent" option and list all of your household members. This allows the USPS to intercept mail coming to your current home and forward it to your PMB. Please note this cannot be reversed, so consider your options carefully.

Within a month, your credit report will likely show this new address, as will premium services such as LexisNexis and CLEAR. This is desired. We want your name associated with this new ghost address. We want your trail to start throwing people toward a mail receiving company instead of a physical location where you reside. This is just the first step, but a big one.

From this point forward, you should give out your new PMB address in situations when you would have otherwise given a PO Box or home address. Exceptions to this include your current driver's license, vehicle registration, and insurance. We are not there yet, but this will be explained later. Think of your new PMB as a PO Box that happens to be far away from you. When you receive a notification of new mail, and want to have it sent to you, it is time to consider your mail forwarding strategy. Most people who use this type of service are not privacy-minded. They simply have the mail from their PMB sent to their home, a friend's house, or another address with associations to them. I urge you to consider a more private option. I never have my PMB mail forwarded to any address where I actually reside. This may be overkill and paranoid, but for good reason.

In 2017, a client notified me that her stalker had contacted her recently, identifying her current home address. This seemed impossible to me. I had taken every precaution. There was no reference to her address online, and her name was never associated with her residence. It was only after he was arrested and interviewed that I found out the mistake that was made. She was having her PMB mail sent directly to her house. He called the PMB provider, requested to schedule a mail delivery on her behalf as her husband, and politely asked where the previous shipment was delivered. The employee read the address back to him with no hesitation. This is a reminder that all PMB companies carelessly give out sensitive details if anyone asks.

This was an extreme privacy violation and should have never happened. Almost all PMB companies have policies prohibiting this, but we are all human. We make mistakes, and are prone to social engineering attacks. I took responsibility in this case, as I did not make it clear

enough to never have your PMB mail sent to your home. You should have a plan for the final destination of your forwarded mail, and this will vary for different scenarios. If you travel constantly like I do, sending your PMB mail to a hotel is ideal. It is a temporary location that will not be applicable to you long term. This can get tricky if you stay in hotels under an alias (as discussed later). If you use your real name, this is fairly simple.

Earlier, I explained a CMRA option, such as the UPS store. These are great for receiving your PMB mail. If you choose this route, I encourage you to find a store located a town or two away from your residence. Getting too close could reveal more information about your home than you desire. This provides a safe local storage area for your mail.

Let's recap our current situation. You have a box at a UPS store under your real name. This is located fairly close to you and is a place you can have any mail sent. You also have a PMB that collects important mail in your real name and forwards to your UPS box. This can be used for situations that typically block CMRA services, such as banks and credit cards. These are the only two addresses where any mail should be delivered in your true name.

While these may not seem like the traditional ghost addresses used in previous decades, they are much more powerful. In 2012, I possessed a ghost address in the southwest portion of the United States. It was a physical structure, somewhat abandoned, but could be used for official purposes. Eventually, the building was sold and I no longer have access to it or any mail sent there. Any shared building services disappeared, leaving me stranded. There are niche communities that have much more intense options such as mail drops in storage closets or back rooms with dedicated street addresses. However, these are quite expensive and only best used short-term. A PMB is a permanent solution which includes benefits unavailable within other privacy-tailored services. Later, I explain how to use this address on your vehicle registration and driver's license. It can become your confirmed physical address, yet you will never step foot at the location.

Escapees Update: Numerous readers contacted me stating that Escapees has inconsistent pricing and can be a wildcard. I encourage you to research Americas Mailbox, which is also in South Dakota. For some, it may be a better (and more affordable) alternative. I explain how I use their service later in the Private Employment chapter. There are benefits to each service, and you should do your own homework. I know many people who have replicated the instruction here with Americas Mailbox as their provider, and have been happy with the service. The only benefit of Escapees is the dual Texas and South Dakota options.

International Considerations: Most countries possess some sort of postal box delivery option. UPS stores can be found abundantly within the United States and Canada. Most European post offices provide various levels of rented boxes. I encourage you to investigate all options within your country of residence.

Chapter Two

Private Mobile Devices

An important step toward completely disappearing is updating all online devices and accounts. Some privacy enthusiasts will tell you that you cannot possess a cellular telephone and still expect any privacy. They have a point, but that is unrealistic. If I informed a client during an initial meeting that he or she could never use the internet again, I would have no more business. My goal is to allow you to enjoy the benefits of technology, but while providing minimal legitimate data to the companies that benefit most from your usage.

Throughout this entire book, please remember that it is designed for the reader in an extreme situation. I will assume that your physical safety is in jeopardy, and that making any mistake is life or death for you. I will treat you like a client who is running from a homicidal former lover that is determined to kill you. I will never consider costs of products, as your safety is more valuable.

I should present the bad news now. If you want extreme privacy, you need all new devices. Your current laptop, cellular telephone, wireless router, and anything else that connects to the internet must go. Clients will ask me if they can simply reformat the drive or hard reset the mobile device, and my answer is always no. Consider the following argument.

Assume that you are a hardcore Apple user. You have a MacBook laptop and an iPhone device. Every Apple product possesses an embedded serial number. This number is associated with your Apple account. Both mobile and laptop devices constantly communicate with Apple servers, supplying the identifiers associated with your devices. Hard resetting (wiping) an iPhone does not reset the serial number. Apple still knows who you are. Creating a new Apple ID for use on these devices does not help. Apple maintains a log of all Apple accounts connected to any device. A court order to Apple, or a rogue employee, can immediately associate your new account to your old, and all of your accounts to all of your hardware. This includes location data and IP addresses. There is simply no way around this. This also applies to most Microsoft and Google products.

Therefore, we obtain new equipment. It is time to replace your mobile device. For my clients, I arrive with the new equipment in order to ensure it is not associated to them at the time of purchase. I pay cash at an Apple store, provide no personal details, and walk out with clean equipment. My image (barely visible under my cowboy hat) is stored on their surveillance system for years, but is not the client's presence. If you plan to buy new hardware with cash,

you may want to find a nominee that does not care about privacy to go in the store and make the purchase on your behalf. During a phone call to an Apple store on my podcast, a manager admitted that every store's surveillance footage is routed to a central collecting location, and stored for an undetermined time. I assume forever.

Some advocate for buying used devices in order to further confuse the systems that collect user data. I do not endorse this. You never know what you are buying. What if the previous owner was a drug kingpin being monitored by the DEA? A court order to Apple shows the DEA agent that the device is now being used by a new account. They would have the legal authority to monitor you. We can prevent this extremely rare situation by purchasing new equipment.

We should probably have the Apple vs. Google discussion. There are likely hardcore Android users reading this that refuse to use an Apple product. They refuse to pay the "Apple Tax" by switching over to another ecosystem. I get it. I am not an Apple fanboy, but I believe the operating systems and hardware on the Apple platform are more secure and private than anything by Microsoft or Google, including Android. I do not like the constant data transmissions that Apple collects and stores about your device and usage, but it is not as bad as the data collection and usage from Microsoft or Google products.

I could fill many books with the unique steps taken to replace all of my clients' hardware and online accounts, but it would likely bore the majority of the audience. Instead, I will abbreviate as much as possible, focusing only on the key elements of each phase. This section is intended to be a "crash course" for the client that is ready to start over and begin a new private life, leaving all connections to previous devices and accounts behind. This will be presented in several breakouts for each type of device. These sections will be simplified, and there are many rabbit holes that can be further investigated online through the resources on my website at **https://inteltechniques.com**.

Overall, this is not a digital security book, it is a privacy guide. However, I want to acknowledge that you cannot have privacy without digital security and vice versa. There are unlimited ways to configure countless mobile devices, laptops, desktops, operating systems, applications, and anything else with a digital display screen. The next two chapters present only the mandatory changes I implement during a full privacy reboot. You will likely possess numerous additional devices that are not mentioned here. Please use the underlying messages within these chapters to make the best decisions about your own digital life configurations.

Let's start with the most important device to replace, your cellular telephone. If you apply only one piece of this book toward your life, I believe it should be a new anonymous mobile device with anonymous service. It is the single tracking device that we all purchase and voluntarily carry with us everywhere. We should make it as private as possible.

Private Cellular Telephone Crash Course

My clients each receive a new telephone with new anonymous service activated. Unless they absolutely insist on an Android phone, I issue new iPhones by default. I believe the privacy and security of an iPhone is far superior to any stock Android device. Additionally, my clients are usually most familiar with the iOS environment. I purchase the number of phones required with cash at an Apple store and leave with the phones sealed in boxes without accepting Apple's activation and setup services.

I create new Apple accounts for each phone through the Apple website from a desktop or laptop computer. I provide a random generic name, forwarding email account, random hotel address and telephone number, and a secure and unique password generated by my password manager (more details on all of this later). I then use these credentials on the device in order to complete the setup process upon booting. You will need internet access via Wi-Fi during this process. If you have already configured your home firewall with dedicated VPN, then you can connect to that network. If not, you should use public Wi-Fi and never touch your unprotected home network to any new device. This will also be discussed in great detail later. If you plan to purchase apps, obtain a prepaid iTunes gift card with cash from a grocery store. This is usually not necessary because you should possess minimal applications and only those absolutely necessary.

For extreme privacy, this device should never be configured from your home. Most phones have location services, Wi-Fi, Bluetooth, and cellular connectivity enabled by default. This could expose your account and associate it with your residence. I will explain in a moment how I isolate my phone from my home. I usually prefer to configure a new device at a location far from the home of the client.

Immediately disable all iCloud services within the device. This will prevent accidental exposure such as emails, contacts, calendars, and notes from being stored within Apple's cloud storage. While I do not recommend using Apple's stock iOS applications for any of these services, it is easy to upload data unintentionally. You can access these settings from the iOS Settings app > Apple Account > iCloud. You should have the option to completely sign out of iCloud and the final result should display "Off" within this menu. Hopefully, you were never signed in.

Some may question my distrust of iCloud. A more appropriate claim would be that I don't trust any cloud storage services for my clients. We have all heard about various breaches which exposed celebrities' personal photos and email messages. These occurred due to the convenience of free cloud storage. The only way to truly prevent this is to block any data from leaving the device itself. I will discuss solutions in a moment. Most of my clients are highly targeted due to their fame, so I insist on completely disabling iCloud, or any other online storage solution.

The next priority is managing the privacy settings of each application. You must give your applications reasonable access to only the settings they need in order to perform their desired task. Navigate to Settings > Privacy and conduct the following modifications.

- Location Services: Turn to the "Off" position. Change this only when in need of a mapping service. Disable individual permissions if you plan to use this feature.
- Contacts: Limit the applications which should have access to your contacts. Services such as communications apps must see your contacts in order to connect you to other people, but other apps should not have access.
- Calendars: If you do not use the stock Calendar app (I do not), then this can be disabled within every application presented.
- Photos: If you never share photos through any apps, it is safe to disable this within every program. It can be enabled if you change your mind.
- Microphone: This should be limited to the applications which truly need access to the microphone to perform their intended function, such as voice messaging applications.
- Camera: This should be limited to the applications that truly need access to the camera to perform their intended function, such as messaging applications which you wish to share photos and videos from your camera. Disable any app which should not have the authority to access your camera.
- Health: Disable completely.
- Homekit: Disable completely.
- Motion & Fitness: Disable completely.
- Siri: Disable and delete all Siri options and data at the following locations:
  Settings > Privacy > Analytics & Improvement > Improve Siri & Dictation
  Settings > Siri & Search > Siri History > Delete Siri & Dictation History

Under Settings > Touch ID & Passcode, select Change Passcode. The default option is a maximum of six numbers, which I believe is insecure. Select the Passcode Options and then Custom Numeric Code. This will allow you to set a longer passcode. I recommend a minimum of twelve numbers. Many people ask about the security of the Touch ID option. I do believe it is secure, and Apple does not receive an image of your fingerprint. Your device creates a mathematical value based on the print, and only looks for a match when it is used. It is only as secure as your passcode, since either can unlock the device. Your decision to activate Touch ID is personal, and most of my clients demand it. I only ask you to consider the following threats.

- Forced Print: If you are placed under physical duress, you could be forced to use your finger to unlock a device. This is extremely rare, but I have had clients who were victims of kidnapping and abduction. These unfortunate incidents weigh heavily on this decision.

- Legal Demands: Some courts have ruled that providing a passcode is not always required as part of a search warrant to search a device, but a fingerprint is. You can refuse to tell your code, but may be physically forced to give up your fingerprint.
- Apple Face ID: I would never consider using this. Although Apple does not store your image, it has been proven vulnerable using images of faces to unlock the device.

As I stated previously, I never use cloud storage for sensitive information such as personal photos and videos. However, I respect the need to possess a backup of this data, especially when our mobile devices likely create and store every image we capture. Since most clients possess a new iPhone and Apple computer, I encourage them to manually backup all content via USB cable. The default Apple application for photo backup is Photos, but I prefer not to use it. Instead, I use the stock application titled Image Capture. This minimal software does not attempt to connect to Apple servers and has limited functionality. Upon connecting an iPhone to an Apple computer, I conduct the following.

- Launch Image Capture and select the iPhone in the upper right.
- In "Import To" option, select the folder on your computer which will store all images.
- Select "Import All" to copy all images and videos to the computer.
- If desired, select all images, right-click, and permanently delete from the device.

You now have your photos and videos on your computer, and I suspect (hope) you are conducting backups of your data to an external device (a tutorial is in the next chapter). By maintaining all of your personal data locally on machines in your possession, you completely eliminate the ability to "hack" into your iCloud and steal your content. You are not bullet-proof yet, but an attack would be extremely targeted and difficult. Note that connecting your new iPhone to your new Apple computer creates a known connection of these two devices with Apple. The risks are minimal since both devices are new with no association to your true identity.

Now that your device is configured with your new Apple account, your privacy settings are tweaked, and your device is more secure, you will need cellular service. In major metropolitan areas, I use Mint Mobile as the provider. Mint is a T-Mobile reseller, and only offers prepaid plans. I choose them because they are very affordable, do not require user verification, and allow prepayment up to a year. At the time of this writing, the lowest monthly unlimited plan was $15 including a free SIM card. I only need the data, as my clients will never use their real T-Mobile issued number for calls or texts.

You can obtain SIM cards from Mint directly from their website, Amazon, or Best Buy. The cards are free if you purchase a package directly from Mint and $5 for two cards if you purchase from Amazon. I purchase dozens of 2-packs from Amazon using an anonymous

account and ship to an Amazon Locker (more on that later), but this may be overkill for your needs. If you only need one or two devices activated, I recommend purchasing the Mint Mobile Starter Pack online from Amazon or in-store from Best Buy. The following are two recommended strategies.

Best Buy: If you are near a Best Buy store, this is the easiest and most private option. Most stores carry the "Mint Mobile $5 Prepaid SIM Card Kit" with a SKU of 6310600. At the time of this writing, the cost was $1.00 and each included $5.00 in Mint Mobile credit. I have been able to purchase dozens at a time.

Amazon: Purchase an Amazon gift card with cash from a physical store, such as a grocery store. Create a new account on Amazon using alias information and an address of a hotel near your location. Apply the gift card to the account and purchase the Mint Mobile Starter Pack. Choose a nearby Amazon Locker for the delivery address. Once your cards arrive, obtain them from the locker.

After you possess a Mint Mobile SIM card, install the Mint Mobile app on the device you recently configured. This should be done away from your home. If possible, use public Wi-Fi. Insert the SIM card and activate the card through the app. This provides you one week of free service to ensure the coverage is acceptable to your needs. It is using T-Mobile service, and I have found the coverage much better than years past. Once you are convinced that Mint Mobile will work for you, select a package within the app. I use very little data, so the 3GB LTE (unlimited at slower speeds) is plenty for my needs. You can prepay for three, six, or twelve months. The longer you commit, the cheaper the price. The lowest package can be purchased for $15 monthly at the yearly commitment. The upcoming chapter on anonymous purchases offers payment options.

Now that you have a new device with a new data plan, you are set. Install only the apps you need, and proceed with private use. Since you should never use the number provided from your cellular company, you will need a way to make and receive standard telephone calls. I currently use **MySudo** (mysudo.com) for most non-secure communications, such as incoming and outgoing telephone calls. This app provides up to nine profiles, and each profile possesses a unique telephone number, email address, and contact list. This service allows me to possess multiple phone numbers on one device, and each can be used for incoming and outgoing calls and text messages.

MySudo does not need your name, email address, or telephone number. The installation is unique to your hardware. MySudo only knows you by this "fingerprint", which has no association to your true identity. You should be able to obtain a free trial, and purchase any premium plans anonymously using the methods discussed later. In the interest of full

disclosure, I was an advisor for, and currently possess shares of the parent company, Anonyome Labs. I explain more about my usage of MySudo later in this chapter.

Many readers may be asking why I never use my number assigned by the service provider. I believe that you should never know the number assigned to the phone and never give it out. There are many reasons, but I will present some strong threats.

Friends & Family: When you give your telephone number to your friends and family, they will likely store it in their contacts and associate your name with the entry. Someone will then download a nefarious app which requests access to the contact list, sending the contacts to online databases which can be queried. We have seen this with several apps in the past, including caller ID services such as TrueCaller and Mr. Number, which shared private contact details with the world. Lately, services such as Twitter and LinkedIn are the bigger concern. Have you ever received an email from LinkedIn asking you to connect with someone you knew? This happens when that person agrees to share their contacts, including email addresses and telephone numbers, with the service. Twitter also wants to obtain these details from any members willing to share them. It only takes one instance to make your cell number publicly attached to your true name. Giving out Voice Over Internet Protocol (VOIP) numbers, as discussed later, can be easily burned and replaced, eliminating the concern of this threat.

SIM Swapping: If I know your true number and I want to take over your account, I can perform a SIM swapping attack. This transfers your number and account from your current device to my device. I am now you. If you use your true number as part of two factor authentication (2FA), I now have that second factor required for login. It is much more difficult to takeover a VOIP number than a standard cellular number.

Tracking: If I know your cell number, I have the one piece of data needed in order to identify your device and location history. This is all stored by your cellular provider, but a court order, data breach, or social engineering attack could easily identify your whereabouts at all times. A VOIP number does not have the connection to your provider necessary in order to retrieve this data.

Logging: Every major cellular telephone carrier logs every call, text message, and data transaction which occurs on your device. Furthermore, they log your location during all activity. Most of this information is kept for years and is available to employees, criminals, law enforcement, and the public whenever a data leak occurs.

Regardless of your threat model, you are prone to becoming the victim of at least one of these issues. I hope that you now possess an interest in eliminating these threats. Since I never use my cellular number for any communication, I need better options ready on my device.

Secure Messaging Crash Course

You should now have a new device that has no connection to you. It possesses prepaid cellular service with no name attached. Since you do not use the number provided by Mint Mobile for any communications, there is no history of your calls and messages. If I wanted to attack you through your mobile device, I have no information to begin my hunt. All of your outgoing calls are made through MySudo, which does not know your true identity. While any mobile telephone is a tracking device which always possesses some type of digital trail to the owner, you have created numerous layers of privacy which will keep you protected from traditional attacks and monitoring. We now need to harden your communications.

Secure Messaging: There is nothing I can say about secure messaging applications that has not been said elsewhere, and I suspect that anyone interested in privacy has already adopted a favorite service. However, a book on privacy would not be complete without mention here. Standard SMS text messaging leaves a huge amount of metadata within the systems of your cellular provider, and they can access the content of the messages. Cellular companies store years of this data, which can then be released intentionally or accidentally. My requirements for a secure communications service include the following.

"Zero knowledge": This means that the provider cannot allow the content of the communications to be intercepted or accessed by any internal employee or third-party. Trusted providers have no ability to view the contents of your communications because the level of encryption from your devices prevents them from any ability to access your data.

Message Expiration: SMS messages leave a history with cellular companies. Secure communication services give you more control. Reputable services allow you to set an expiration of your messages. Once the expiration passes, the messages disappear on your device and the recipient's device. This is not bulletproof, as screen captures or exports can create additional copies, but it provides a basic layer of protection.

Encrypted Voice Calling: When I need to talk with a client, I only use services which provide true encrypted calling. This prevents wiretapping and other technologies from intercepting and recording my call. There is still a risk that the other party could record the conversation, but interception by a third-party is very unlikely. Compare this to a traditional telephone provider which can intercept any call.

There are a large number of secure messaging types of apps emerging. I will disclose those which I use and recommend, in the order of my preference.

Wire: This is my preferred secure messenger over all others. While not perfect, it offers features currently unavailable in all other providers. Wire is free for personal use, and has

adopted a large audience of users within the privacy community. An email address is required to create an account, but can be a forwarding account such as a Blur or AnonAddy masked email address. A ProtonMail address may be more appropriate for long-term access. Wire has native applications for iOS, Android, Windows, and macOS. If you are using any other system, you can also connect via their website. Regardless of your connection, you can communicate via text, audio, and video across all platforms. This is a rarity.

Wickr: This was one of the earliest secure communications applications and it works very well. I have numerous contacts that use this service and it is often at the top of the list for new clients seeking only text and voice options. The voice calling feature can be used from the desktop application, and a mobile device presence is not required. I typically seek services which I can use from my desktop when desired.

Signal: There are many things I do not like about Signal, but it seems to still have the largest user base. Therefore, I must keep it within my arsenal. I would rather communicate over Signal than SMS text, and many people in my life possess Signal as their only secure option. Signal requires a telephone number in order to create an account which is a huge privacy violation. You must give out this number in order to communicate with others securely. If you choose to use Signal, you should create an account associated with a VOIP number, such as a MySudo or Google Voice number. I prefer MySudo for this if you have access to an account. Google Voice should be your second consideration. Once you have an account, you have access to secure text, audio, and video communications. Signal has a desktop application, but it only supports text communication.

Session: I really like Session. It is truly anonymous in that it assigns a random username (Session ID) and never asks for a telephone number, email address, or any type of verification. The reason it is below Signal is because of low adoption (it is a much newer service). If my contacts jump into Session as a form of secure messenger, I would begin transitioning more clients to it. At the time of this writing, it only allowed text communication and no voice or video calling options.

MySudo: MySudo offers free secure communications within their network. This includes text, audio, and video. If the majority of your contacts have MySudo, then this may be the only option you need. It is lowest on the list because of lower adoption and no ability to place calls through a browser or desktop application. Fortunately, the Android version was released in 2020. If this brings in a flock of new users, I would happily place this service above Signal.

Overall, you should adopt whichever secure service will be used by those in your circles. If no one in your life is using secure communications, you have an opportunity to select the best service for your needs and start recruiting people to it. If everyone in your life already uses a specific service, jump on board.

VPN Crash Course (Mobile)

Virtual Private Networks (VPNs) provide a good mix of both security and privacy by routing your internet traffic through a secure tunnel. The secure tunnel goes to the VPN's server and encrypts all the data between your device and that server. This ensures that anyone monitoring your traffic before it reaches the distant server will not find usable, unencrypted data. Privacy is also afforded through the use of a distant server. Because your traffic appears to be originating from the VPN's server, websites will have a more difficult time tracking you, aggregating data on you, and pinpointing your location. I break this down further in the next chapter.

Virtual Private Networks are not a perfect anonymity solution. It is important to note that VPNs offer you privacy, not anonymity. The best VPNs for privacy purposes are paid subscriptions with reputable providers. There are several excellent paid VPN providers out there and I strongly recommend them over free providers. Free providers often monetize through very questionable means, such as data aggregation. Paid VPN providers monetize directly by selling you a service, and reputable providers do not collect or monetize data. Paid providers also offer a number of options that will increase your privacy and security. I currently endorse ProtonVPN as my "daily" VPN, and PIA on firewalls (explained later). I will always maintain a direct link to the most affordable subscription on the "Links" page on my website. The current rate for PIA is $42 per year while ProtonVPN ranges from free (slow) to $95 per year (fast). Both include unlimited use and connection to multiple devices. Configuration of a VPN on your mobile device can be extremely easy or somewhat challenging, depending on your level of paranoia. Let's approach this from three levels.

Basic: For most readers, and almost every client I have consulted, I recommend sticking with the standard application provided by a VPN company. Whether this is a larger provider such as PIA and ProtonVPN, or a smaller supplier such as Mullvad, the apps provided directly from the company should suffice for your needs. These can be downloaded from the App Store or Google Play. Once installed, simply provide your account credentials and launch your VPN connection. This was my personal choice for many years.

Intermediate: Many VPN apps are closed source. This means that we cannot truly know what the app is doing behind our backs. While most reputable VPN companies have our best interests in mind, we must always be cautious. In 2019, PIA announced they were being purchased by a company called Kape Technologies. Kape has been accused of injecting spyware/malware into its apps in the past, which has worried many PIA users. This is one of many reasons I encourage people to research the OpenVPN application. This free open-source mobile app allows you to configure multiple VPN clients within one location. If you have subscriptions to more than one service, you can configure each within the app and select

the desired provider and server upon each connection. Configuration will require some research, but most VPN companies provide explicit instructions for this option.

Advanced: The downside to the two previous options is that a third-party service is required for your VPN connection. You must install some type of application in order to execute the VPN connections. Another option is to manually configure your VPN through your mobile device's system settings. With iOS, I can specify the exact VPN details and make a connection without any third-party software. In my experience, PIA refuses this type of connection, but ProtonVPN encourages it. At the time of this writing, full instructions were available at https://protonvpn.com/support/protonvpn-ios-manual-ikev2-vpn-setup. This option uses the IKEv2/IPSec protocol, which is built into iOS. Most will agree that OpenVPN provides slightly more secure encryption, but it requires a third-party app. IKEv2/IPSec does not require an app, but has slightly weaker encryption.

What should you choose? If the terms OpenVPN, IPSec, and IKEv2 mean nothing to you, then you should stick with the basic option. It offers a very secure environment, but you may give up a bit of privacy in rare scenarios. Fortunately, both ProtonVPN and PIA have made all of their applications completely open-source. This makes it much more difficult to hide malicious programming within the code. If you do not want to install third-party apps and want to use a VPN directly through your mobile operating system, the advanced option may be desired. I encourage you to test them all and learn the protocols. Overall, ANY of these options, while using a reputable provider, beats no VPN at all.

My VPN policy is quite simple, but my opinions about VPN companies can be complex. Any time that I am connected to the internet from my laptop, desktop, or mobile device, I am connected through my VPN. I know that my internet traffic is encrypted and originating from an IP address not associated with me. I never deviate from this policy. I believe that every reader should consider a paid VPN. In a later chapter, I will present a more hardened home solution for a constant VPN in your home. In the next chapter, I share more insight on the use of VPNs for privacy.

What do I use? I rely 100% on ProtonVPN through their app on my mobile device and laptop(s) while I am traveling. I trust them more than most commercial options and I believe their business model is the most transparent. Being hosted in Switzerland provides some aspect of privacy from vague government intrusion, but international servers could always be compromised. I only rely on PIA for my home firewall as a catch-all masking service with great speed. I provide explicit details on that later in this book, and any updates in regard to recommendations will be posted on my website at **https://inteltechniques.com/vpn.html**. Throughout the remaining chapters, I will present much more information about VPN usage and services.

Device Backup and Restoration Crash Course

Once your device is configured exactly as desired, you may wish to make a full backup to an Apple computer. This allows you to easily restore your configuration to a new device if something should happen to your current phone. This has saved me much frustration after a device participated in a full wash cycle while left in a coat pocket. This requires you to open iTunes on your new Apple computer, connect the mobile device via USB, and conduct the following.

- Click the small phone icon in the upper left.
- Click Summary in the left menu.
- Under Backups, click Back Up Now.

If you are using macOS Catalina, you will find this option in the Finder application. The process should be the same. This will create a clone of the operating system and configuration within the iTunes app (or Finder) on the computer. If you do not possess an Apple computer, you could use iTunes installed to a Windows machine. If you want extreme privacy, you could set up a Windows virtual machine on a Linux host, disable all internet access to the Windows VM, install iTunes within the Windows VM, and connect your mobile device to the iTunes installation. Regardless of the way you do this, having a backup of your mobile device will be a huge benefit if you ever need to replicate your configuration onto a second device. This is vital for my clients, as I will not be with them when a disaster happens.

In late 2019, I purchased a new iPhone for myself. Usually, I would make a fresh start with a new Apple ID, but I wanted to test my backup strategy. I turned the device on; chose the iTunes connection option; connected it to my MacBook Pro; launched iTunes; selected the device; and chose the option to "Restore Backup". Within a few minutes, I possessed a new iPhone which was identical to the previous device. All software, configurations, and settings were present. I insist that all of my clients possess a valid backup of their device, ready for easy restoration.

You may have noticed that my iPhone backup and restoration instructions require the Mojave edition of macOS instead of Catalina. I have had many problems with Catalina, and avoid it for now. Upgrading will eventually be unavoidable. Currently, Apple supports Mojave and provides security patches. Catalina blocks any 32-bit applications and enforces aggressive changes in the disk structure. It has "broken" many applications. By the time you read this, Catalina may be old news. I plan to stay on Mojave until it is no longer supported by Apple (likely after 2023).

Secondary Device Crash Course

Your new private iPhone may be all you need in regard to a mobile device. Most people carry it with them everywhere they go and leave it connected to the mobile network at all times. I believe this is risky behavior and a desire for extreme privacy will require you to take more extreme action. My primary mobile device has never entered my home and has never connected to a cellular tower within five miles of my house. While unlikely to happen, it prevents my phone from announcing my home location. If someone did figure out my mobile number, and paid a bounty hunter to locate my device, it would not lead anyone back to my home. The last known location would be a busy intersection with no connection to me. You can accomplish this and still possess a mobile device in your home with all of the communication apps you need with the following instructions.

When I am traveling, my phone is always by my side and is my primary means of secure communications. When I return home, things change. When I am about five miles away from my home, at a very specific location, I drop my device into a Faraday bag. This shielded pouch prevents any signals from reaching or leaving my phone. It stops communications with cellular towers. The device stays in this bag until I am at least five miles from my home heading out on another trip. Since the phone is never connected to any network while near my home, it cannot reveal the location of the device (or my home).

While at home, I can still possess a mobile device for my secure communications. I use an iPod Touch for this. The iPod Touch possesses the same iOS operating system as the iPhone. It connects to my wireless network in the home (behind a firewall with VPN as discussed later) and has internet access. It possesses a unique Apple ID never used on any other device. My secure communication apps, such as Wire, work the same as on my primary phone. MySudo possesses the same telephone numbers for incoming and outgoing calls. Since I do not use any Apple services on either device and rely on trusted third-party applications, Apple does not know that I am the owner of both devices.

The hiccup with this plan is the one-time setup of the communications. In order to replicate an installation of MySudo, and share the same numbers across both devices, both devices must be active at the same time. I must scan a barcode from my primary device with my iPod Touch. Both devices need internet access during this process. Therefore, I set all of this up on public Wi-Fi before taking the iPod Touch to my home. This is a one-time exception.

First, I enable power on the iPod Touch at any library with free Wi-Fi and allow my cellular telephone to be connected to a cellular data connection. I configure everything on the secondary device as needed, which will require access to the primary device to allow these connections. I then "forget" the Wi-Fi network on the iPod Touch. An optional step here is to tell the device to forget all networks, if desired. I then turn it off completely.

Upon arriving home (with my cell phone in a Faraday bag), I connect the iPod Touch to my home Wi-Fi (behind a VPN firewall as explained later) and it never leaves the house again. This secondary device replicates all communications options I need. Aside from lack of a cellular-provided number and service, it appears identical to my "phone".

Another issue with this plan is the installation of Signal on the secondary device. Unlike username-based services such as Wickr and Wire, Signal relies on a telephone number. Furthermore, it only allows usage on one mobile device at any given time. However, it provides a desktop application which can be used on multiple machines. Therefore, my secondary mobile device (iPod Touch) does not possess my primary Signal account, but my primary laptop does. I can send and receive text messages over Signal while using this laptop. This prevents me from making calls through my primary Signal account while at home, but it presents an opportunity to introduce people to better communication alternatives. Almost all of my secure calls from home are placed over Wire or Wickr. If a client insists on a call through Signal, I can connect through a secondary Signal account from the iPod Touch. I just need to let them know the call may be coming from an unusual number.

I insist on preventing any devices from connecting to any cellular network while in my home. These connections can immediately identify someone's location. The iPod Touch has no cellular connectivity. It never leaves the home and never connects to any other network. I think of it as my landline which only functions in the home. If you possess an anonymous telephone with prepaid service and an anonymous Wi-Fi only device, both of which have no connection to your identity or each other, you have an amazing layer of privacy protection.

If you go through the troubles of obtaining an anonymous home as discussed later, these steps are vital so that you do not expose yourself. Airplane mode is not enough. System updates often disable airplane mode on reboot. It only takes one accidental connection to create a permanent record of the location of a device. These steps prevent unintentional exposure that could ruin all of your hard work.

Some readers of the previous edition expressed concerns of Apple eliminating the iPod Touch from its lineup of mobile devices. Fortunately, they released a 7th edition in 2019. This device supports the current version of iOS (13). Based on previous support models, I expect the latest iPod Touch to receive support updates through 2023. You should note that all iPod Touch models lack Touch ID, Face ID, 3D Touch, NFC, GPS, an earpiece speaker and a noise-canceling microphone. However, all communication functions work well with a set of earbuds which contain an in-line microphone (such as those included with most older iPhones).

Faraday Bag Selection and Testing

I insist on thoroughly testing any Faraday bags I purchase. Over the past ten years, I have acquired at least five bags which failed to prevent signals from entering or escaping the sleeve. Some may place their device in a bag, seal it, and call the phone number of the device to see whether it rings or forwards the call to voice mail. I do not believe this is an accurate test as you are relying on the signal strength of the nearest tower. A test in a rural area may be successful while that same test in an urban city could fail. Also, a failed call due to poor coverage may provide false assurances of the functionality of the bag. Instead, I rely on Bluetooth as my primary signal test. I can control the test better and apply strong local signals. The following is my routine with a $15 small, portable, battery operated Bluetooth speaker.

- Connect the mobile device to the speaker via Bluetooth.
- Play music from the device to the speaker.
- While music is playing, drop the mobile device into the bag and seal it.
- After the previous test, with music playing, drop the speaker into the bag and seal it.

In both scenarios, the audio should stop a few moments after sealing the bag. With some devices, the audio may play a while before stopping due to buffering. Now we should test other wireless signals.

- Connect the mobile device to Wi-Fi.
- Stream an internet radio station from the mobile device through the internal speaker.
- Drop the mobile device into the bag and seal it. The audio should stop.
- Disable Wi-Fi and enable a cellular data connection.
- Stream an internet radio station from the mobile device through the internal speaker.
- Drop the mobile device into the bag and seal it. The audio should stop.

In my experience, a poorly constructed Faraday bag is more likely to block cellular or Wi-Fi signals than nearby Bluetooth frequencies. I have yet to see a successful Bluetooth blocking test reveal that cellular frequencies were allowed. Therefore, Bluetooth is my baseline to detect the function of all Faraday bags. I also believe you should test the other connections as explained above. In my opinion, a Faraday bag should never be used before thorough testing. If your bag begins to show wear, repeat these tests. If your bag does not function properly 100% of the time, there is simply no point in using it at all.

Telephone Usage Crash Course

Now that you have an anonymous telephone and isolated Wi-Fi only "Home" phone, we should have a conversation about usage on both. I believe that we should all use mobile devices as they were originally intended, as a means of necessary communication. I do not believe privacy-conscious people should ever consider a mobile phone as an entertainment device. It should not be used for games, video streaming, or extensive web browsing. We should be very reserved with the applications installed on these clean devices. My two devices are almost identical as far as application presence. While they have unique Apple IDs, the usage and setup are quite similar. Each device contains the following apps.

Telephone: As explained previously, I rely heavily on the MySudo app on both devices. It allows me to replicate my account on my second Wi-Fi device so that I can make and receive calls and text messages from all nine of my profiles and numbers. If you are unable to use MySudo, or prefer to host your own VOIP solution, I explain another strategy in Chapter Sixteen. While everyone will have their own use cases, my partial usage is as follows.

- 1: Personal (Real Name): This is for friends and family who do not use secure communications (telephone only). When they adopt MySudo, I can still use this line for encrypted communications.
- 2: Google Voice Forwarding (Real Name): All of my old Google Voice numbers forward all calls and text messages to this single number (explained later). I can now answer all 35 of my old numbers in case a call should come through. This is beneficial when friends and colleagues from many years ago try to contact me through an old Google Voice number which I have given them. Google knows these were all me.
- 3: Home (Alias Name): This name, number, and email address are unique to anything that involves my home. Utilities, services, maintenance, neighbors, and all house-purchase paperwork connects to this profile. When that line rings, I know to answer as my home alias.
- 4: Business (Real Name): When I need to deal with any business-related phone call, I use this profile. This number has been leaked to business lookup websites. The email address is used for any business-related registration I must complete which will ultimately send me spam.
- 5: PMB (Real Name): You previously learned how a PMB in another state can help create a great layer of privacy. This number is local to the area of my primary PMB and allows me to really "sell" it.
- 6: Social (Alias Name): As mentioned previously, being anonymous does not mean you can't live a normal life. This number is used for any social activities near my home. New friends I meet under my new alias have this number for me.
- 7-9: Due to my own privacy concerns, I will not disclose the specifics of these account.

Email: I use the standard ProtonMail application and connect my premium account to each device. This allows me to send and receive secure emails from multiple ProtonMail addresses as well as accounts associated with domain names which I own. I explain ProtonMail further in the next chapter.

Secure Messengers: The messengers mentioned previously are acceptable on all of my devices. I keep them all ready in case a client has a preference.

VPN: My clients all have the ProtonVPN app on their devices, but I choose to program my ProtonVPN settings manually and use the devices' built-in VPN option. At home on Wi-Fi, I connect to my firewall with forced built-in VPN and a VPN connection is not necessary on the iPod Touch (as explained later).

These apps allow me to communicate securely via email, encrypted text, encrypted voice, encrypted video, and traditional telephone service. I have every avenue of communication covered, and each device allows full use through all of my accounts. The end user does not know which device I am using. My cellular service provider knows absolutely nothing about my activity, only the amount of data used. T-Mobile also has no record of any calls or text messages, and does not know the name attached to the account.

Web Browser: Your choice and configuration of a web browser on your desktop computer is very important. Your options within the Apple iOS operating system are limited. Apple mandates that any third-party browsers rely on its own rendering engine. This means that every browser on an iPhone is still using Apple's code, regardless of the brand. Chrome, Firefox, and every privacy-themed option is still using Apple's internal browser software. However, I believe there are better alternatives than the stock Safari application. I prefer Firefox Focus for all web browsing from my mobile devices. Firefox Focus provides three key features which I find useful.

- Easy History Removal: A trash can is present next to the URL bar at all times. A single click on this icon removes all internet history, search queries, and active pages from the application. This is much easier than opening Apple's Settings menu, scrolling to Safari, and then clicking the "Clear History" option.
- Tracking Protection: Firefox Focus offers embedded tracking protection from various online trackers and analytics. Furthermore, you can allow Firefox to force Safari to share these blocking settings. This way, when an application opens a link within Safari, you have some additional protection.
- Simplicity and Speed: I believe Firefox Focus offers the most simplistic and speedy web browsing experience out of all of the popular options.

Number Porting Crash Course

Now that you have a new mobile device with new anonymous service, you likely need to make a decision about your previous device and service. You could cancel the account and lose the number forever; keep the plan and check the old device occasionally for missed calls and messages; or port your old number to a Google Voice account. I prefer porting over all other options, but let me explain why before providing instructions.

If your old device is out of contract, you have the right to discontinue service. If it possessed a prepaid cellular account, you can suspend the service and simply stop using that plan. Most readers likely possessed a device with a contract through a traditional carrier. If you are still under contract, it may be more affordable to keep the plan until it expires. If it is a newer contract, it may be more affordable to pay an early termination fee. Regardless, at some point the plan will be discontinued. When that happens, you lose all access to that number. Any incoming calls and messages will be lost, and you will not be able to use that number for any sort of verification process, such as calling your bank to make changes to an account.

I do not believe you should ever lose a telephone number that has ever been important to you. When you change your number and start providing a VOIP number, such as a MySudo or Google Voice number, it is unlikely you will remember to contact everyone that has your old number. This can lead to missed calls from old friends or lost text message reminders from services you forgot to notify. Worse, someone will eventually be assigned your old telephone number if you do not maintain it. That stranger will start receiving calls and messages meant for you. Think about any time you obtained a new telephone number. You likely received messages meant for the previous owner. A mischievous person could have some fun with that.

I will assume that you are ready to port over your old number to a new permanent holding place. If you are out of contract, you are in the clear. If a contract exists, you will be held responsible for any early termination fee. I have found that notifying your current carrier and providing a new physical address as your new home which cannot receive their service is sufficient for waiving any fees. I have yet to find a carrier that can provide service to the following address, in case you find this information to be helpful.

10150 32nd Avenue NW, Mohall, ND 58761

The most important first step is to not cancel your service with your old carrier. If you do this, the number is lost and you have no way to port it over. Your account must be active and in good standing in order to port your number to another service. Once you successfully port the number over, that action will terminate the original account. This may make more sense after we walk through the process together. In the following scenario, you have recently

purchased a new device, executed new prepaid service, and you still possess your old phone with the original service still active.

As you may recall, I am not a fan of Google products from a privacy perspective. However, Google Voice is our current best option for porting numbers. MySudo would be preferred, but they do not support number porting at the time of this writing. You might look into that option as it could be available by the time you read this. Once we have the process in place, there will be no need to log in to the Google account, and you will never do so from your new clean device. Google will receive information about your communications through their service, but I do not see it as any worse than your previous telephone carrier possessing the same data.

The first consideration is to identify which Google account to use for the porting. If you have never had a Google account, you have no choice but to create a new one. Many people may think that a new account should be mandatory for this procedure, but I have a different view. Google can be cautious when it comes to new accounts. If you create an account from a VPN using a burner email address, Google might find this suspicious and suspend the account until you upload government identification proving your identity. I find this invasive. I respect their need to block usage from spammers, scammers, and other crooks, but I do not want to have my own account suspended. If you already have a Google account established in your true name, and your old phone was also established in your true name, I see no reason why you should not pair these together.

Remember, our goal is to configure a system to receive calls and messages from a number that was already associated with your true identity. Connecting this to a Google account under your true identity does not gain or lose much privacy at this point. I would rather attach your old number to an aged Google account that has very little risk of being suspended due to questionable activity than to connect it to a brand-new account which will be scrutinized by Google.

If you have an old Google account in your name, I suggest using that. If you have no account, I would create an account in your true name. This may sound ridiculous from a privacy perspective, but if it gets suspended, you have a much better chance unlocking it when you are the person with whom it is registered. It will receive extremely minimal use, and Google will collect very little information from it. Let's get started.

- Find your billing account information from your current service provider, such as your account number and PIN. You need this information to complete your port request.
- Within a web browser while protected by your VPN, navigate to voice.google.com.
- Sign in with your Google account credentials if you are not automatically logged in.

- If you haven't used Google Voice on your account before, set up a new Google Voice account. You'll be prompted to pick a new number, but your ported number will soon replace it, so it won't matter what that number is. You can use your old cell number as your verification number, as it is still active on the old device.
- At the top left, click "Menu", "Legacy Google Voice", then "Settings".
- Click the "Phones" tab.
- Next to your current number, click "Change / Port".
- Select "I want to use my mobile number". Follow the onscreen instructions to set up your new number and pay. Google will charge a $10 fee for the porting. You might be charged a $20 fee to port your mobile number to Google Voice from some mobile service providers, such as Verizon or AT&T. Prepaid credit cards or Privacy.com cards should be accepted for payment without any issue.
- Continuously check the status of your number porting. Numbers typically take from 48 to 96 hours to port.
- Don't cancel your phone plan until Google notifies you the port is complete. To verify the port, they will call your phone with a code. After the port is finished, your service provider will cancel your phone service.
- If you have multiple numbers on the original account, check with the service provider first to find out about their policies. If you want to keep the plan and get a new mobile number, confirm that with the service provider.

Once you see your old number which was previously attached to your cellular telephone appear as your new number in the Google Voice account, the porting is complete. Test this by completing the following steps.

- While logged in to your Google account, navigate to mail.google.com.
- Navigate to www.callmylostphone.com and enter your telephone number.
- On the Gmail screen, you should see an incoming call.

There is no need to answer this call, you just want to make sure that the number can receive calls through Google Voice. You are finished with this step. If anyone from your past calls your old number, you have a way to receive notification of the call. This applies to text messages as well. You have control of the number. If you need to make a call from that number, such as to prove your identity to a bank, you can make calls from the Gmail or Voice pages while logged in to the Google account in a web browser. Having the ability to occasionally check the Google account may be all you need. Personally, I do not like logging in to Google products, so I take advantage of their forwarding options, as explained next.

Number Forwarding Crash Course

I mentioned previously that one of my MySudo profiles is for Google Voice forwarding. Over the years, I have accumulated many numbers from Google Voice. Some of these are heavily associated with my true name. As an example, I used a Google Voice number when I worked as a Detective at a police department. We were all required to disclose our cell numbers on a callout list, and I only provided a Google Voice account. To this day, I hear from former colleagues through that number. Many of them assume it is my cell number, and I have no need to correct them. While I have moved all of the people with whom I continuously communicate over to better options, this Google number still receives a lot of activity. The following explains how I interact with these numbers without using the official Google websites or apps.

First, let's assume that you are a MySudo user and that you have a profile dedicated to Google Voice numbers. After that, I will present a completely free option. In MySudo, you have a random telephone number of 202-555-1111 and email address of google@sudomail.com assigned to the profile. Any calls to that number will ring your phone through MySudo and incoming emails will be received within the MySudo application. Your telephone carrier and manufacturer will not know of these calls or messages. For extra protection, disable iOS Call Integration within the Calls option in the Settings menu. This prevents calls from appearing in the Apple call history.

- In your web browser, navigate to voice.google.com, click on the left menu, and select "Settings". Your Google Voice number should be the old cell number which you ported into Google.
- The "Linked Devices" section should either be blank or possess the same number as your previous cell number. Remove any numbers within this block by clicking the "X" next to each.
- Add a new linked number and enter the MySudo number mentioned previously (202-555-1111).
- In the "Messages" section, ensure that messages are forwarded to the Gmail account connected to this profile.
- In the "Incoming Calls" section, ensure that calls are enabled.
- In the "Calls" section, ensure that "Get email alerts for missed calls" is enabled.
- In the "Voicemail" section, ensure that "Get voicemail via email" is enabled.

You may have noticed that Google allows voicemails and missed call notifications to be delivered to the forwarding telephone number. I have found this to be unreliable, and only trust the email option. Let's pause and think about what is in place now. If anyone calls your old number, the call is routed through Google Voice and then to your MySudo number. Your

phone will ring as normal and you can accept the call. The caller ID will show the number calling you. If you decline the call, the caller will be sent to your MySudo voicemail. If you simply do not answer, it will be sent to the Google Voice voicemail. If he or she leaves a message on the MySudo voicemail, you will see it within the app. If the message is left within the Google environment, your Gmail account will receive the audio and text version of the call. If someone sends you a SMS text message to this old number, it will be received in the Gmail account as well. Now, let's forward those messages in order to prevent checking the Gmail account at all.

- Navigate to gmail.com while logged in to the account associated with the old number.
- Click the gear icon on the right and select "Settings".
- Click the "Forwarding and POP/IMAP" option in the upper menu.
- Click "Add a Forwarding Address" and enter the email associated with your MySudo profile as discussed earlier (google@sudomail.com).
- Google will send a confirmation email to your account.
- You should now have the option to select "Forward a copy of incoming mail to" and choose your MySudo email address in the drop-down menu. Choose "Delete Gmail's copy" and save your changes.

Now, when someone leaves you a voicemail or sends you a text message to the Google Voice number, it will appear in your MySudo profile and Google will delete the original after 30 days. You can now receive calls, voicemails, and text messages from your old number within your MySudo application without ever logging in to Google again. You can also respond to text messages via your MySudo email address and the recipient will only see the previous cellular number that is now assigned to Google Voice.

It is vital to test all of these options before relying on them. If you have MySudo, test all calling and texting options from another profile and make sure that everything appears as desired. If you do not have MySudo, let's repeat the entire process with alternative options.

- In your web browser, navigate to voice.google.com, click on the left menu, and select "Settings". Your Google Voice number should be the old cell number which you ported into Google.
- The "Linked Devices" section should either be blank or possess the same number as your previous cell number. Remove any numbers within this block by clicking the "X" next to each.
- In the "Messages" section, ensure that messages are forwarded to the Gmail account connected to this profile.
- In the "Calls" section, ensure that "Get email alerts for missed calls" is enabled.
- In the "Voicemail" section, ensure that "Get voicemail via email" is enabled.

If anyone calls your old number, the call is routed through Google Voice and then immediately to voicemail (unless you are logged in to Google Voice via web browser). If he or she leaves a message, your Gmail account will receive the audio and text version of the call. If someone sends you a SMS text message to this old number, it will be received in the Gmail account as well. Now, let's forward those messages in order to prevent checking the Gmail account at all.

- Navigate to gmail.com while logged in to the account associated with the old number.
- Click the gear icon on the right and select "Settings".
- Click the "Forwarding and POP/IMAP" option in the upper menu.
- Click "Add a Forwarding Address" and enter your ProtonMail email address associated with your real name (this will be discussed in the next chapter).
- Google will send a confirmation email to your account.
- You should now have the option to select "Forward a copy of incoming mail to" and choose your ProtonMail email address in the drop-down menu. Choose "Delete Gmail's copy" and save your changes.

Now, when someone leaves you a voicemail or sends you a text message, it will appear in your ProtonMail account and Google will delete the original after 30 days. You cannot receive calls, but will be notified of voicemails and text messages from your old number without ever logging in to Google again. You can also respond to text messages via your ProtonMail email address and the recipient will only see the previous cellular number that is now assigned to Google Voice. Again, this should be tested before actual use.

I have replicated this process across all of my old Google Voice numbers. This may seem sloppy, as Google now knows I am the owner of all of the accounts. My stance on this is that it likely does not matter. Google probably already knows. Their heavy use of browser fingerprinting, analytics, and IP documentation allows them to know when people use multiple accounts. Since I no longer have these numbers as part of my normal usage, I consider them all "burned" and only wish to have the ability to receive any notifications. If you call or text any of my old numbers, my primary device receives the communications through MySudo. I never use these accounts to make any outgoing calls or texts, only incoming content from those that do not know my true number(s).

There is one small annoyance with this plan. You can no longer call out from your old Google Voice numbers unless you log in to a Google account. I try to avoid this. If I really need to place a call, and the caller ID on the other end needs to be an old Google Voice number, I will use **FireRTC** (firertc.com). This service allows you to create outbound VOIP calls from within your web browser. Accounts are free, and you are limited to one telephone number per account. However, the telephone number assigned to you is not what you will use as your caller identification. When configuring your account, you can choose any legitimate telephone

number as your caller ID. This allows you to appear to be calling from a known Google Voice number if desired.

There are many uses for this service. Imagine that you contact your credit card company in reference to your account. The cellular telephone number that they have on file is your previous Google Voice account that you do not wish to access. For security purposes, they mandate that you contact them from a known number to protect your account. You could change the caller ID within FireRTC to match your previous Google Voice number and repeat the call. This could also be used to prevent unwanted return calls by choosing an outgoing public number such as large library or corporate office. Remember to never use this for anything illegal or to attempt any type of fraud. A proper court order to FireRTC will immediately disclose your IP address and account information. Please be responsible.

Android Options

All of the content in this chapter preceding this point is the advice I present to my clients. While I find iOS the easiest option for a general audience, I respect that there are situations when an Android device is justified. In fact, I have an Android with me during all of my travels, which I will explain in a later chapter. Until then, let's consider a few reasons you may not want an Apple phone.

- Apple has a completely closed-source operating system. We have no idea what is going on behind the scenes. While I believe it is in their best interest to protect their customers, the entire ecosystem could be one huge piece of malware collecting all of our data for nefarious use.
- You cannot opt-out of the Apple ID requirement when using an iPhone. Installing any apps or updates requires you to possess an account, which documents and stores many details about your device, account email, apps, podcasts, and other usage. This is unsettling, and one reason I insist on purchasing and registering phones anonymously.
- Apple devices are expensive. While you can usually find a decent refurbished model for half of the price as new, you will never find devices cheap enough to be used as true "burners".

I absolutely refuse to use or provide a stock Android mobile device from a major manufacturer such as Samsung or Motorola. The data collection from Google is intense and the stock apps are full of privacy invasions. When I need to use Android, I rely on a custom rom called **LineageOS** (lineageos.org). Chapter Sixteen provides an example of a complete installation and configuration process.

Linux Phones

In 2020, I saw the emergence of two privacy-respecting Linux telephones from **Purism** (puri.sm) and **Pine64** (pine64.org). Both offer the ability to physically disable the cameras, microphones, and communications hardware. This alone is a huge feature for us. Both devices possess Linux operating systems which provide enhanced privacy and security. On the surface, these devices sound perfect. Unfortunately, this is not the case. Both devices rely on your cellular service provider for calls and communication. VOIP is possible, but extremely limited. Google Voice and MySudo will not work with these devices. At the time of this writing, Wire, Wickr, Signal, ProtonMail, Tutanota, and Fastmail do not support the operating systems. This eliminates the vast majority of features I require in a mobile device. I truly hope that the future presents a scenario where a Linux phone meets all of my needs. Until then, I do not recommend these devices.

Camera and Microphone Blocking

Our mobile phones are designed to make life simple and fun. Most devices possess two cameras and numerous microphones. Selfies, high resolution photos, and speakerphone calls are simple thanks to the hardware present. However, these features can be used against us. Malicious software can enable a microphone or camera without our knowledge. The most recent iOS and Android operating systems possess protections from this type of misuse, but bad things can still happen. In 2019, Facebook was caught secretly enabling the front camera of mobile devices while users were viewing their feeds within the app. Most social network apps circumvent security software by convincing you to authorize the necessary permissions to access your microphones and cameras. If you possess apps from Facebook, Amazon, and other providers, you will likely find that they all have unlimited access to your microphone and camera. Because of intentional and accidental exposure, I embrace camera and microphone blockers for the devices of all clients (and my own).

Camera blockers are easy. Much like a laptop, you can cover your mobile device cameras with black electrical tape or a dedicated sticker. Both the EFF and Silent Pocket offer reusable stickers designed to block embedded web cameras. The EFF versions may be a bit large for your mobile device, but the Silent Pocket option provides multiple sizes and colors. At a minimum, I encourage people to consider covering the front-facing "selfie" camera, as blocking the rear camera would also prevent any intentional photos. Due to paranoia, I keep both of my cameras covered until I need to use them. There are sliding metal products which easily enable the camera when desired, but I have found all of these to be poorly made and unreliable.

Microphone blocking can be tricky. Modern iPhones possess four unique microphones, none of which can be easily disabled. If a rogue app or virus began listening to your conversations,

you would never know. The only fool-proof option would be to destroy each microphone, but that would make the device much less usable. Our best consideration is to "plug" the microphones. First, we must understand how microphones are chosen by system applications.

Think about your current mobile device. If you make a call and hold the phone up to your ear, you likely hear the other person through the small speaker near the top. The other party hears you through a microphone near the bottom. If you enable the speakerphone, you now hear the person through the speakers at the bottom. They hear you through the microphones at the bottom. Now imagine plugging in a set of earbuds with an inline microphone. You now hear the other person through your earbuds and they hear you through the microphone within the cable. The operating system of the device detects all of this activity and adjusts the input and output based on your actions. Let's focus on that inline microphone attached to your earbuds.

When you attach any type of headset which includes a microphone, your device detects this and switches the default microphone to the headset. It does not disable the other microphones. It only "listens" to the microphone which is plugged in. Now imagine if the microphone within the headset was broken. If you made a call through these earbuds, you would hear the other party, but they would not hear you. The device is only listening for the microphone plugged into the phone. If you have an old set of earbuds you do not wish to use again, consider the following experiment. Cut the cable directly below the in-line microphone, but above where the cable splits for each ear. The remaining earbud will still work, but there is no microphone. The phone believes a microphone is present due to the plug structure. The phone enables the missing headphone microphone as the default and no one will be able to hear you on calls. This is the design behind a microphone plug.

Fortunately, you do not need to keep a pair of destroyed headphones plugged into your device in order to achieve these same results. Many companies offer "mic plugs" which virtually disable the working microphones of the device. Figure 2.01 (left) displays one of these options, a standard 3.5mm microphone plug made by **Mic-Lock** (http://amzn.to/2B6QvXw). This unit is larger than other flush-fitting models, but I have found it to be more reliable. When you plug this device into your phone, it tells the operating system that you just inserted a pair of headphones with an inline microphone. Therefore, it makes this new mic the default option and tells all applications to listen to it if audio is needed. Since a microphone does not actually exist within this device, only silence is delivered.

Newer mobile devices present another problem. Many do not possess traditional headphone jacks, and only offer a Lightning or USB-C connection. You have a couple of options if you want to block default microphone access in these devices. If you already have an adapter for standard headphones, you could attach a microphone blocker to this adapter, and insert the other end of the adapter into your phone. This should work, but would need to be tested.

Alternatively, some microphone blocking companies are now creating plugs for these new connections. Mic-Lock offers a Lightning port to 3.5mm headphone port adapter with the in-line microphone disabled. Figure 2.01 (right) displays this device. You plug it into the phone and plug your earbuds into the adapter. The advantage with this unit is that you could wear headphones (with or without a microphone) and disable the default microphone at the same time. The disadvantage is that a long adapter sticks out when only desiring the microphone blocking element, as seen in Figure 2.01 (right).

There are numerous "L-Shaped" and miniature microphone blockers which are much smaller and fit flush to the device. I avoid these for two reasons. First, many of these units unintentionally activate Siri or other apps because they send a virtual "long press" to the device. This causes battery drain and undesired Siri activations. Second, the smallest devices are often lost when removed. The larger plugs are easy to find and control. Also, their presence is obvious and you will know that you are protected.

Obviously, there are ways to defeat all of this protection. A truly malicious app or virus could be configured to ignore a headset microphone and force activation of internal mics. While possible, it is not very likely. I never consider these plugs to stop an extremely targeted attack. However, I believe they are valuable in blocking the common threats from social network apps and shady advertising practices. If you believe you would never be targeted for surreptitious video or microphone monitoring, consider the accidental "butt dial".

Most of us have accidentally dialed someone from our mobile device while placing it into our pocket or a bag. That person can then listen to us without our knowledge. A microphone blocker prevents this unintentional transmission of audio. Have you ever participated in a group FaceTime call or conference chat and accidentally pressed the option to activate your device camera? I know I have. Fortunately, my camera blocker stopped any video transmission to the other participants. Hopefully, you will never need to rely on the protection of a camera or microphone blocker. Proper protection eliminates threats and provides peace of mind.

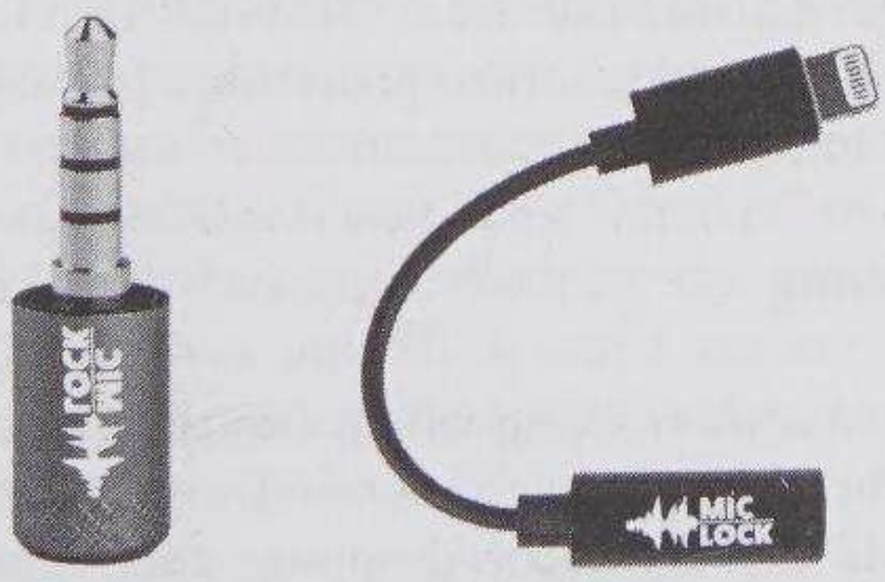


Figure 2.01: Microphone blocking devices.

Mobile Device Firewall

When you launch an application within your mobile device, several network connections are executed. By default, we do not know much about these transmissions. Obviously, communication apps need to connect to servers in order to function. However, what else is happening behind our backs? Is your favorite "privacy app" sending data to social networks without your consent? I was surprised to learn of the number of privacy violations occurring when popular applications where opened. This is the reason I rely on a firewall on all of my devices. Let's start with the iPhone.

Lockdown (lockdownhq.com) is a simple firewall which is free and completely open-source. Installation from the App Store is easy, but the software is not activated upon installation. Enabling the Firewall adds a virtual VPN configuration to your device. This connection intercepts all local network traffic and provides an option to block any undesired transmissions. Clicking on "Block List" reveals various collections of invasive tracking services which are commonly present within mobile applications. This includes tracking URLs from Facebook, marketing companies, and user trackers. My preference is to "Enable" every list. Next, it is time to test.

Open an application on your device, allow it to load, and close it. Open Lockdown and identify the blocked connections within the "View Log" option. This will disclose any suspicious traffic being blocked from that application to the tracking recipient. Repeat the process for each app on your device to discover any concerning activity. Anything you see in the log was blocked by the firewall. When an application attempts to send data to tracking companies such as Facebook, the transmission is blocked. You can also add any custom domain desired. I allow Lockdown to run at all times, and visit the log weekly to preview the content being restricted. The additional battery drain is minimal without any noticeable impact.

The business model of Lockdown is their paid VPN service visible within the firewall app. I find it to be overpriced and a bit "generic", but I understand the need to make money on that service in order to keep the firewall free. Android users might consider **NetGuard** (netguard.me) which seems to provide similar protection. It is free, open-source, and does not require "rooting" in order to function.

Wi-Fi & Bluetooth Tracking

There is a new trend in customer tracking which concerns me. Many retail stores, shopping malls, and outlet centers have adopted various wireless network monitoring technologies in order to follow customers throughout a shopping area. These rely on your Wi-Fi and Bluetooth emissions from your mobile device. When you enter a store, your signals are collected and stored. As you move around, various sensors attempt to identify your exact

location and length of time within a specific area of a store. If you leave without purchasing any items, you might be tracked by the neighboring store and your pattern is helpful to their customer analytics. This may sound too futuristic, but it happens every day. Random spoofing features being adopted by Apple and Android help with this invasion, but companies always find new ways to track us via the signals our devices broadcast at all times.

My solution to this is simple. The Bluetooth and Wi-Fi signals on my travel phone are always off. If you are using an iPhone, tapping the network options on the home screen will not suffice. You must go to the Settings application and manually disable both Wi-Fi and Bluetooth. Many will resist this, as keeping these connections enabled is very convenient. Your device will immediately connect to your car stereo and switch over to your work Wi-Fi when you enter the building. However, this comes at great risk. As stated previously, my travel phone never connects to any public Wi-Fi (or my home's network). I only rely on the cellular data package and I do not use my device for internet browsing or video streaming. When I want to connect my device to my car stereo, a USB to Lightning cable works flawlessly, and without requiring any wireless signals. Please eliminate any technologies which makes you easier to track.

Pagers

I received my first pager in the mid-nineties. It was amazing. I could be anywhere, and receive a ten-digit number requesting a callback. This sounds archaic today, but the technology was fascinating at the time. This eventually led to alpha-numeric pagers which could deliver full text messages from standalone devices connected to a landline. This may seem unnecessary today, but the technology still exists and pagers are still available. The biggest consumer is the medical industry, where pagers work well when cellular signals cannot reach portions of hospitals. I have had only one client request a pager for daily use, but I know of a few people in my circles who continue to carry these devices. I will explain some extreme use cases that may encourage you to investigate further.

The benefit of pagers over cellular telephones is coverage and privacy. Your traditional mobile device is constantly communicating with multiple cellular towers, all of which are documenting your location. Contrary, pagers receive communications without sending an exact location back to the tower. The outgoing message is sent like a "blanket" over the entire coverage area. This also occurs on a much lower frequency, allowing the signals to reach further than a traditional cellular carrier. This is over-simplified, and I am not a pager frequency expert. Overall, pager companies do not know exactly where you are, but can still get messages to you wirelessly.

There are three main types of pagers for our use, and each may have benefits and limitations for your needs. Each of these can possess various protocols for message delivery, and all have security weaknesses. It is common for network penetration testers to intercept pager messages.

Numeric: I can call your pager number, enter a telephone number, your device notifies you of the number entered. I also have the option of leaving you a voicemail message. If I do this, your pager presents your own number to you in order to call it and receive the message.

Alpha-numeric: I can send you a text message via email, internet, or standalone unit. I can also replicate the features of a numeric pager.

Two-way: You can receive messages via the previous options, and an attached keyboard on your device allows you to respond.

My client that desired a pager only required a numeric unit. He was an extremely high-risk target who did not carry a cellular telephone at all times. He subscribed to my Faraday bag usage and only removed his device when he needed to make a call. However, he had concerns about his children. The school was aware of threats made to the entire family, and had strict orders to contact my client if anything suspicious happened. The school possessed the number to his pager, and would leave a message when they needed to reach my client. His wife also had this number. If a voicemail was left on his account, he received notification of this almost instantly. I must confess that I do not possess or require a pager, nor do many people I meet. For those that need extreme privacy and security, it is a viable option.

Summary

Hopefully, you now possess a new phone with absolutely no public connection to you. It has service through a T-Mobile reseller which does not know your true identity. The service is paid through either prepaid cards or your Privacy.com account (explained later). The phone has never connected to any cell towers near your residence thanks to your new Faraday bag. There is no cellular location history associated with your home. Your secondary iPod Touch is the only mobile device used in your home and it possesses a unique Apple ID, while never leaving the house. Your old number forwards to Google Voice and eventually reaches both your primary and secondary devices. This all happens with zero knowledge from your cellular carrier.

All mobile telephones are tracking devices. We can never change that. When there is no association to your true identity, the threat of this tracking is minimized. There will always be a digital trail, but these tactics make you a very difficult target.

Chapter Three

Private Digital Life

Your computers disclose a lot of details about you, your family, and your interests. The sites you visit can disclose the city where you live. The security of your systems, or lack of, decide whether you will become victim to a ransomware attack or allow a criminal to eavesdrop on your activity. The unpatched applications you use may expose you to automated attacks which turn your computers into servants for criminal organizations. All of this can be avoided, but not with the stock settings provided to you by default. You must intentionally seek and change many configurations in order to possess true digital privacy. We should start with the primary computers used by anyone in your home or business.

In order to achieve extreme privacy, your choice of computer operating system is very important. My preference for my own use is Linux Debian installed directly on the computer (not a virtual machine). I always push tech-savvy clients toward a full-time Linux solution. If you fit into that group, you don't need me to tell you how to set up a Linux machine. Since Linux is often met with great resistance from my clients, and most demand a "traditional" operating system, my second choice is an Apple macOS device. Apple constantly collects user data for their own use, but supposedly does not sell this data to third parties (yet).

Most of my clients are familiar with Mac products, and I believe they possess much better overall security than a Microsoft Windows system. Some clients are stuck in the Microsoft environment and insist on a Windows machine. In the next several pages, I will explain my recommendations for each of these options, and explain each step I take before handing a computer to a client. The only system I refuse to incorporate into a client's new digital life is a Google Chromebook. There is simply no way to achieve any privacy within that operating system.

Similar to the previous chapter, a recurring theme is that a new device is optimal instead of trying to sanitize an existing computer. I briefly mentioned the risks of using recycled or reformatted phones in the previous chapter, but I would like to dive deeper into this concern here. The moment you connect any Apple computer, tablet, or smartphone to the internet, Apple collects all information associated with the Apple ID account (name, address, email, credit card, etc.). Apple then appends this record with the unique serial number of your device, all hardware details, and the IP address of your internet connection. Apple now has a nice dossier on you and your device. This information can be seen by Apple employees, anyone

with a court order requesting these details, or potentially through a data breach at Apple. As you continue use of this product, Apple stores much of your activity such as your desired podcasts, email contacts, wireless networks, and dozens of additional metrics.

If you were to format your computer and start over with an alias name, email, and home address, Apple would still see the unique serial number and have the ability to connect the user accounts together. Microsoft collects similar information through their Telemetry "feature", and Google products are even more invasive. Aside from corporate invasions into our data, I consistently meet clients which have various keyloggers, malicious software, and monitoring applications intentionally installed on their devices by stalkers, former lovers, and other adversaries. Because of this, I always demand that high-targeted clients receive all new computer equipment. I will begin with the most common option I see lately, which is Apple computers.

Feedback from the previous edition of this book was that this chapter is overwhelming. In my previous books, the topics presented here were stretched out over numerous chapters containing explicit details. I have attempted to condense some of these topics for easier digestion. Anything mentioned in this chapter can be further researched online, and you will likely find yourself diving into many new rabbit-holes. Remember, this book is about the advice I present to my clients desiring a complete privacy reboot. This chapter can be taken in small doses and I encourage repeated reading of the information. I present considerations in the following eight categories, with a very brief summary of each.

- **New Computer Configuration**: This section provides explicit tutorials in order to properly configure a new computer for ultimate privacy and digital security.
- **Password Manager Usage**: This section explains the importance, installation, usage, and archiving of a locally-stored password manager.
- **Account Security**: Account hardening with proper two-factor authentication is vital for overall security. The details here will ensure you are not compromised.
- **Encrypted Storage**: You possess tons of sensitive data. This section explains how to properly protect your photos, videos, documents, and other valuable content securely.
- **Web Browser Configuration**: Your browser is the most common tool used against you online. Malicious ads, trackers, and other annoyances must be blocked.
- **Virtual Private Networks (VPNs)**: Your internet provider issues you a unique number which can track your online habits. This section stops that practice.
- **Email Strategies**: While extreme at times, this section explains how to properly (and easily) create unlimited email accounts which all forward to one inbox.
- **Travel Considerations**: Border crossings, international flights, and other travel presents new challenges to the privacy enthusiast. These considerations should help.

New Apple Computer Crash Course

As stated earlier, my preferred computer for most clients is an Apple macOS device. It is targeted by malicious online attacks much less often than Microsoft Windows, and is considerably more secure than Windows, especially with default settings. Most clients are already familiar with the Mac environment and comfortable with the operating system. The following is my mandatory list of configurations and modifications when issuing a new Apple computer to a client.

Apple ID: When first booting a new or reformatted MacOS device, you will be prompted to provide an Apple ID, or create a new Apple ID account providing your name, physical address, and email address. You have the option to bypass this requirement, but you will be prohibited from using the App Store. This eliminates many software options and disables the ability to update and patch your App Store applications. An Apple ID is NOT required to download and install system updates. I no longer attach an Apple ID to my Apple computer, and I encourage my clients to do the same. If you never associate an Apple ID to your device, Apple has no easy way to store any of the activity to a profile. It also prevents accidental iCloud activation. I encourage you to skip the Apple ID creation process and proceed to the FileVault step in the next pages. You can always add an account later if absolutely required. However, if you know you will need the App Store or iCloud (neither of which I recommend), use the following procedure for obtaining an anonymous account. I repeat the following for clarity. An Apple ID is required for iOS devices, but not macOS computers.

Please note that Apple will store the IP address of the internet connection you use to complete this process. In an optimal scenario, you will be connected to either a public network (such as a coffee shop) or behind a home firewall (as explained later). Ideally, you would never give Apple your true home internet IP address. When I configure hardware for my clients, I occasionally do so from the Apple store where the devices were purchased (with cash). Since there is already a trail to where the computer was purchased, I see no harm in using the in-store Wi-Fi to complete the following tasks.

When prompted to provide an active Apple ID, click the "Set up later" option near the top. Confirm this decision if prompted. Apple will then demand a full name, account name, and password. Choose something generic for the full name such as Office Laptop which will also populate a similar username. Choose a strong password which you can remember, but is not in use anywhere else. More details on passwords are provided later.

Next, choose "Customize Settings" and be sure to disable location services and all analytics on the following screens. If prompted, choose to set up Touch ID later. You should now see your desktop and have full access to the operating system. However, you still do not have the ability to update stock apps or download any software from the App Store. In order to do

this, Apple demands that you possess an Apple ID account. If this is desired, open the Safari web browser and navigate to appleid.apple.com and select the Create Your Apple ID option. This specific process is very intentional.

When you create an Apple ID through traditional methods such as the MacOS installation screen, Apple is very likely to demand a cellular telephone number as part of the process. They will also send a verification text to that number which must be entered to complete the registration. We do not want to provide a number to Apple. When registering online through their web portal, Apple is much less likely to demand a cellular number. When registering through their web portal using the Apple Safari browser, you are even less likely to be required to provide a phone number. This is why I always create Apple ID accounts via the Safari browser, even if they will be used on an iOS device. You will still be required to provide a name, address, email account, and telephone number. However, none of this is verified. I choose the following for clients.

- Name: Generic name such as Jane Smith
- Address: Any large hotel address in the country of residence
- Telephone: Number associated with the chosen hotel
- Email: Valid ProtonMail account created exclusively for this purpose
- Password: Secure password generated by a password manager (explained later)

Any time I configure a new machine for a client, I also create a new ProtonMail email address. This free address will only be used in association with the device, and allows me to confirm the address as active, which almost always eliminates any demand for a cellular telephone number. This email address can be used later to register third-party software if needed. I will discuss secure email later, but know that you should have a dedicated account for this purpose.

Once you have your Apple ID account created, use the credentials to sign in to the App Store. This will allow you to update any stock applications and install new software desired. From the System Preferences menu, launch Software Update and allow your system to apply all updates. Next, launch the iCloud utility. Make sure you are NOT logged in to iCloud. If the login process for the App Store also logged you into iCloud, be sure to sign out on the iCloud screen. Since Apple associates all iCloud content to the dossier created about you previously, we will not use their services for any storage. **I encourage clients to avoid creating an Apple ID for any computer unless it is absolutely necessary in order to use a specific software application.**

You should now have an Apple device which offers full functionality. Apple does not know your identity and you have not provided any personal data through the Apple stock applications. I do not recommend use of the Apple Mail, Contacts, Calendar, iCloud,

Reminders, Messages, Facetime, iTunes, News, Time Machine, or Siri applications. We will use more private and secure options. We only need the core operating system from Apple.

FileVault: The next step I take is to apply full-disk encryption to any new Apple device. This process is extremely easy by opening System Preferences and selecting Security & Privacy. Choose the FileVault option to see the current state of encryption on your device. By default, this is disabled. FileVault is a built-in full-disk encryption utility that uses AES-256 encryption. Enabling FileVault requires you to create a recovery key and gives you two options through which to do so. The recovery key is an emergency, 24-digit string of letters and numbers that can be used as a recovery option should you forget your password. The first option is to store the recovery key in your iCloud account, which is not advised. The second recovery option is the most secure. Your device will display the 24-digit series of letters and numbers. This code is not stored with Apple or in your iCloud account. I copy this key, paste it into a TextEdit word processor document, and save the file into an encrypted container, as explained later. Alternatively, you could store this key in your password manager, which is also explained later.

Once you have enabled FileVault's full-disk encryption, your system possesses an extremely important level of security. The entire contents of your computer's storage can only be read once your password has been entered upon initial login or after standby login. If I steal your device and attempt to extract your data via forensic process, I will only see unreadable data. By default, every computer's hard drive is ready to give up all of the secrets until you apply full-disk encryption.

While we are in the System Preferences, let's make a few more changes. Back in the Privacy & Security option under General, change the "Require password" option to "immediately". This will ensure that your laptop requires a password any time you shut and open the lid. Next, choose the Firewall option and enable it. Note that you may need to click the padlock in the lower left in order to make changes. The firewall blocks incoming connections to the computer. This is especially important if you use public networks.

Antivirus: There is likely no need for anti-virus applications on an Apple device, especially if you practice safe browsing habits. I never recommend commercial anti-virus products for Mac. If you insist on Anti-virus being present, consider ClamAV, an open-source free solution. The following will install Brew and ClamAV to your Mac.

First, you must install a package manager called Brew. This program is very beneficial when there is a need to install programs which would usually already be present on a Linux computer. It also happens to have a pre-configured version of ClamAV ready to go. The easiest way to install Brew is to visit the website brew.sh and copy and paste the following command into the Terminal application (Applications > Utilities > Terminal).

/usr/bin/ruby -e "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/master/install)"

After Brew is installed, type the following commands, hitting "Return" after each line, into the same Terminal application used previously. The first command disables Brew's analytics program, which relies on Google's services.

- brew analytics off
- brew install clamav
- sudo mkdir /usr/local/sbin
- sudo chown -R `whoami`:admin /usr/local/sbin
- brew link clamav
- cd /usr/local/etc/clamav/
- cp freshclam.conf.sample freshclam.conf
- sed -ie 's/^Example/#Example/g' freshclam.conf

These steps will install ClamAV, switch to the installation directory, make a copy of the configuration file, and then modify the configuration file to allow ClamAV to function. You are now ready to update your antivirus database and conduct a scan. Type the following commands into Terminal.

- freshclam -v
- clamscan -r -i /

The first option will download all virus definition updates, and should be executed before each scan. The second option conducts a scan of the entire computer, and will only prompt you with details of found viruses. While it may appear to be dormant, it is working, and will notify you upon completion. All of these commands must be exact. In order to assist with properly copying and pasting these commands, I have created a web page with every step at **https://inteltechniques.com/clamav**.

ClamAV may occasionally present a false-positive report of a virus. Do not panic. Research the file on the internet and identify the issues. If you receive reports of malicious files within email, simply delete those messages. Note that the above scans only SEARCH for viruses, they do not REMOVE threats. If you would like to conduct a scan and automatically remove suspicious files, you must conduct a different command. Please note this could be dangerous, and could permanently remove necessary files. I always run a scan, research the threats found, and execute the following scan ONLY if I am confident the files should be removed.

- clamscan -i -r --remove=yes /

The use of ClamAV on Mac and Linux computers is more about preventing the spread of bad files to Windows users instead of protecting your own machine, but viruses do exist for non-Windows systems. I try to scan my entire drive at least once monthly on all machines.

AntiMalware: Windows users are likely familiar with the need for malware-scanning applications. This is not as necessary with macOS, but there is one malware detection application I highly recommend. **KnockKnock** scans the applications set to persistently run on your machine and verifies they are clean through the online service VirusTotal. If you have malware running on your machine, KnockKnock should detect it (but will not eliminate the threat). Full details can be found at objective-see.com/products/knockknock.html. I run this application weekly, but I have yet to find anything malicious. However, it has opened my eyes to the number of undesired plugins, extensions, and launch items which are snuck into the operating system without explicit consent. The following explains steps to take in order to execute a scan and remove undesired content.

- Download, install, and open the software. Click the "Start Scan" option in the center.
- Research all extensions, plugins, and launch items. Identify anything undesired.
- Click the "show" icon to the right of anything you do not want present.
- If identified as malicious, delete the item. If unsure, rename and move to another location and reboot your machine. This could break any applications requiring the deleted item, but may identify undesired software which is present unknowingly.

Little Snitch: This software, upon first installation, is easily the most annoying application to my clients (and myself), but may provide more privacy than anything else we can install. I already mentioned how Apple constantly collects data from your machine about your usage. Little Snitch can block any outgoing data desired. It acts as an outgoing firewall. Instead of trying to block data from coming in to your machine, it stops data from being sent out. After installation and configuration instructions, I will explain a typical scenario.

- Navigate to https://obdev.at and download the Little Snitch application.
- Launch the program and accept defaults. When prompted, click "Open Security Preferences", then "Allow", and close the "Security & Privacy" window. Your computer will reboot upon successful installation.
- Upon reboot, take the tour of the application. Choose "Alert Mode" and disable the "iCloud Services" option.

If you wanted to be more aggressive, you could have disabled the Apple core services option along with the iCloud Services feature. These two settings block all Apple core services, but may break many things. Since we do not want to use iCloud, disabling that feature is fine. It provides an extra layer of protection in case iCloud should become accidentally enabled. If

you choose to block all Apple services, practically every stock application will refuse to connect to the internet, and you will have issues. We can always make changes later. Let's look at a few examples where Little Snitch should allow and block access to specific applications.

First, launch Firefox. You should immediately be prompted by Little Snitch asking if Firefox should be allowed to send out data to the internet. We want this to happen, so you should select the default "Forever", then "Any connection", and finally "Allow". You should never be prompted about Firefox again.

Now assume that you want to add information into the stock Apple Calendar. This will only be stored on your laptop, and it should not be synchronized to an Apple server or anywhere else. When you open the calendar app, Little Snitch notifies you that the Calendar is attempting to connect to caldav.icloud.com. Even though you are not logged in to an iCloud account, and you have never asked Apple to sync anything for you, it sends data to their servers many times throughout every day. Little Snitch can block this. When prompted, choose "Forever", then "Any Connection", then "Deny". Little Snitch will quietly block these attempts every time. If you only wish to block the domain connecting to Apple, in case you add your own calendar later, you could select the second option, "Only domain icloud.com", as seen in Figure 3.01 (left).

Figure 3.01: Little Snitch menus.

If you click the new menu icon in the upper right of your Desktop, you can select "Little Snitch Rules" and customize every aspect of this software. The window seen in Figure 3.01 (right) highlights my iTunes setting to block all outgoing connections. Double-clicking this entry opens the options for this configuration and allows me to change the setting or delete the rule altogether. This application requires much time for proper configuration. Once set up, you will possess a more private operating system which shares much less data with Apple and other applications. As another example, I have my Mac set to block all outgoing connections to Microsoft when I open Word, Excel, or any other Office application. Microsoft does not need to be notified about my usage.

Note that this free trial is limited to three hours during each boot. After that time, the software shuts off and you are exposed. If you reboot your computer every few hours, this may work for you, but it is not feasible for most users. I highly recommend purchasing this application, as it is affordable and provides a permanent license. I purchased my own copy under an alias name, and receive nothing to promote this product.

OverSight: Another privacy application from objective-see.com (maker of KnockKnock previously mentioned) is OverSight. After installation, you will observe a small umbrella icon in the upper right menu of your Mac. By default, it is now monitoring for any application which attempts to receive input from sound or video devices. In other words, if a program surreptitiously enabled your microphone in order to capture a conversation, OverSight would display a notification. If an application enabled your webcam, OverSight would let you know. While OverSight is free, a paid alternative made by the same company as Little Snitch is called Micro Snitch. I slightly prefer Micro Snitch over OverSight, but both offer the same features.

Regardless of your technology solution, you should always physically cover your webcam with some type of temporary sticker. You may also consider a physical microphone blocker. I previously explained both of these options. You can find links to these products on the "Links" tab of my website at **https://inteltechniques.com**. Other software I occasionally add to a client's Apple machine is as follows.

Onyx (https://www.titanium-software.fr/en/onyx.html): If your Apple operating system is behaving strangely, Onyx may be able to correct the issue. This maintenance program should not be executed on a schedule, and should be reserved for situations of undesired behavior. On occasion, my fonts become corrupted and my menus become unreadable. Onyx fixes this.

VirtualBox (https://www.virtualbox.org): If a client will ever need to launch a Windows machine, VirtualBox is a free virtual machine software application. It is also valuable for testing other operating systems before committing within a designated computer. I explain my usage of virtual machines in Chapter Sixteen.

MacUpdater (https://www.corecode.io/macupdater): This program scans all installed applications and provides a notification if an update is available. While I do not use the program's feature of automatically updating software on my computer, the notice allows me to manually update any outdated software on my own terms.

Carbon Copy Cloner (https://bombich.com): This is the best full-disk backup software I have found for Mac. It allows me to create a cloned drive of my client's machine, which can be used to restore the computer back to the original state it was in during the clone. The clones can also be used as a bootable drive in case the computer operating system is completely corrupt. This is not traditional file synchronization software, which will be explained later.

New Microsoft Windows Computer Crash Course

Many readers may be more comfortable with the Windows environment, and choose it over Apple devices. Most businesses require Windows in order to use specific software or more controlled network management. Some may want a more affordable computer and never consider the overpriced Mac line of products. Regardless of your reason, Windows might be the more appropriate option for you. In my previous books, I presented privacy and security options for Windows 7, which is a much less invasive operating system than Windows 10. Windows 7 will no longer receive support or scheduled security updates as of January 2020. Therefore, I no longer recommend Windows users continue to possess Windows 7 as an operating system. Unfortunately, we must embrace Windows 10.

The good news with Windows 10 is that you can bypass account creation altogether. An active Microsoft account is not required in order to complete the installation and receive important software updates. This eliminates the need to provide Microsoft with your name, home address, and email account. However, there is much worse news. Microsoft's Telemetry service continuously collects the following data, plus numerous additional details, sending it to their corporate servers in Seattle.

- Typed text on keyboard
- Microphone transmissions
- Index of all media files on your computer
- Webcam data
- Browsing history
- Search history
- Location activity
- Heath activity collected by HealthVault, Microsoft Band, other trackers
- Privacy settings across Microsoft application ecosystem

This data would make it very easy to identify you, your location, and all online activity. Microsoft claims this collection of data is only to enhance your experience. I find this invasive, and I will present options to disable much of the data collection. First, we must complete the installation process. If you have a new computer or are reinstalling the operating system, you will be prompted to choose "Express Settings" or "Customize Settings". Choose the custom option which will present many choices for your new system. Disable each option presented on the screen. This will disable some of the most intrusive privacy violations such as the ability to collect keystrokes as you type and sending usage data to Microsoft.

Your computer should now boot into the account creation screen. Choose the Skip this step option to bypass this intrusion. You must now submit a username. Much like the Apple instructions, I suggest a generic account such as Office Laptop and choosing a strong

password which you can remember. If required to provide a "Hint", simply type the word NONE. Your computer should finish the initial boot process. After booting, enter the Control Panel and apply all system updates.

Similar to the Apple configuration, I want to possess full-disk data encryption. My preference for Windows 10 Pro machines is to use Microsoft's Bitlocker. This is a proprietary encryption program for Windows which can encrypt your entire drive as well as help protect against unauthorized changes to your system such as firmware-level malware. If you have the Pro version of Windows 10, you only need to activate Bitlocker in the Control Panel by following the directions, which are similar to the Apple option. Unfortunately, if you have a Windows 10 Home version of the operating system, Bitlocker is not available to you. In this common scenario, or if you do not trust Microsoft to provide your encryption, I suggest using VeraCrypt for full-disk encryption. The following explains the entire process.

- Download VeraCrypt from https://www.veracrypt.fr. Execute the installer and select the "Install" option. You can accept all the default settings in the installer.
- Once VeraCrypt is installed, launch the program.
- Click System > Encrypt System Partition/Drive in the VeraCrypt window.
- You will be asked whether you want to use "Normal" or "Hidden" system encryption. The Normal option encrypts the system partition or drive normally. When you boot your computer, you'll have to provide your encryption password to access it. No one will be able to access your files without your password. The Hidden option creates an operating system in a hidden VeraCrypt volume. You will possess both a "real" operating system, which is hidden, and a "decoy" operating system. When you boot your device, you can enter the real password to boot your hidden operating system or the password to the decoy operating system to boot it. If someone is forcing you to provide access to your encrypted drive, such as a border crossing mandate, you can provide the password to the decoy operating system. In terms of encryption, using "Normal" encryption keeps your files just as secure. A "Hidden" volume only helps if you are forced to disclose your password to someone and want to maintain plausible deniability about the existence of any other files. If you are not sure which you want, select "Normal" and continue.
- Select "Encrypt the whole drive" and choose "Single-boot".
- Choose the encryption standard of the default setting.
- Enter a password. It is very important to choose a strong password which is unique and can be remembered. I will discuss more on this later. VeraCrypt will ask you to move your mouse randomly around inside the window. It uses these random mouse movements to increase the strength of your encryption keys. When you have finished, click "Next".

- The VeraCrypt wizard will force you to create a VeraCrypt Rescue Disk image before continuing. If your bootloader or other data ever gets damaged, you must boot from the rescue disk if you want to decrypt and access your files. The disk will also contain a backup image of the contents of the beginning of the drive, which will allow you to restore it if necessary. Note that you will still need to provide your password when using the rescue disk. VeraCrypt will create a rescue disk ISO image at C:\Users\NAME\Documents\VeraCrypt Rescue Disk.iso by default. You can either create a CD using this image, or simply save the ISO in case of emergency. Note that the file should be saved somewhere other than the drive which is being encrypted.
- When prompted for "wipe mode", choose none, especially if this is a new computer.
- VeraCrypt will now verify everything is working correctly before it encrypts your drive. Click "Test" and VeraCrypt will install the VeraCrypt bootloader on your computer and restart. If Windows doesn't start properly, you should restart your PC and press the "Esc" key on your keyboard at the VeraCrypt bootloader screen. Windows should start and ask if you want to uninstall the VeraCrypt bootloader.
- Enter your VeraCrypt encryption password when your computer boots. Sign in to your device when the normal welcome screen appears. You should see a "Pretest Completed" window. Click the "Encrypt" button to actually encrypt your device's system drive. When the process is complete, your drive will be encrypted and you'll have to enter your password each time you boot your computer. If you decide you want to remove the system encryption in the future, launch the VeraCrypt interface and click System > Permanently Decrypt System Partition/Drive.

After successfully encrypting your drive, you now possess a huge layer of security. If I steal your device, I cannot access your content without the password. If I remove the hard drive and connect it to a secondary forensic machine, I have no way of reading the content. This process may seem like a hassle, but the benefits are worth the effort.

Windows absolutely requires some type of anti-virus solution. I prefer the default Microsoft Defender over any commercial options. Some will say this is reckless as Microsoft Defender collects user data and submits it back to Seattle. This is true, but no more invasive than the other data collection which is default with Windows 10. Basically, Microsoft already knows what you are doing. Microsoft Defender has less overhead than most commercial solutions; it is completely free; it is included with Windows 10; it automatically applies updates from Windows; and it is designed specifically for threats toward Windows 10. Therefore, I prefer it over anything else for Windows 10 users. The default settings are acceptable.

In previous books, I recommended a cleaning application called CCleaner. I no longer use this product because of some unethical practices of its owner Piriform. Some versions of CCleaner contain Ad-ware which has been accused of collecting user metrics. My preference today is to use **BleachBit** (bleachbit.org). BleachBit is very similar to CCleaner, but can be a bit more

aggressive. I select all available options with the exception of "Wipe Free Space". Choosing this would overwrite all free space on the hard drive which is time consuming. BleachBit removes leftover internet history content, temporary files, and many other types of unwanted data. I execute this program weekly.

Next, I strongly advise users to attempt to minimize the amount of data Microsoft collects about your computer usage. I already explained a few options during the installation process, but there is much more content which needs blocked. There are many free utilities which assist with this, but I have found **O&O Shut Up 10** to be the most effective and current. Download the latest version at www.oo-software.com/en/shutup10 then install and launch the software. You will see many individual options which can be enabled or disabled. A red icon indicates that feature is disabled while green indicates enabled. The wording can be murky. In general, anything red indicates that data about that topic is being sent to Microsoft while green indicates the service is blocked. As an example, the first option states "Sharing of handwriting data disabled". The default option is disabled (red). Switching to green tells us that this threat is disabled, and we are protected.

Some may want to play with each individual setting. Most choose a pre-determined level of privacy. In the Actions option at the top, you will see three categories of "Recommended", "Recommended and somewhat recommended", and "Apply all settings". The first option is very safe and applies normal blocking such as disabling advertisement IDs. The second option is a bit stricter and blocks everything except automatic Windows updates, Windows Defender, and OneDrive. The last option blocks everything possible. My preference is to select the "Recommended and somewhat recommended" option, and then enable the Microsoft OneDrive Disabled option. This leaves updates and Defender running.

After you have made your selections, close the program and allow Windows to reboot. Open the application again to make sure your desired settings were maintained. Every time you update the Windows operating system, take a look to see if you need to re-enable your choices here. If you ever have troubles because of your level of protection, you can reverse these changes any time from within the application.

If you want to replicate the abilities of Little Snitch on Windows, check out **Glass Wire** (glasswire.com). If you want to scan for software updates, consider **Patch My PC** (patchmypc.com). Since I encourage clients to avoid Windows if possible, I do not provide a tutorial for either application here. I find these useful, but both feel like bandages blocking holes on a sinking ship. Hopefully, you now possess a system with full-disk encryption, an anti-virus solution, a software update policy, and an overall hardened configuration for your daily needs. These basic tutorials will likely apply to over 95% of this audience. I rarely meet a client willing to ditch Apple or Microsoft completely. However, I refuse to complete a section about new computers without promoting Linux as a primary operating system.

New Linux Computer Crash Course

In 2018, I switched to Linux full-time, and now only use an Apple machine for production (generating press-ready PDF files, website management, recoding training videos, and other tasks which are more difficult on Linux). My daily driver is a Debian Linux machine. However, that is not my recommendation for those new to Linux. If you have a strong opinion of one flavor of Linux over another, I respect your choice and you do not need the following tutorial. If you are new to Linux and desire a version which may provide an easy transition, I recommend Ubuntu. I can hear the sighs coming from tech-savvy readers who disagree, but consider my reasons.

- Ubuntu allows easy access to software packages in a graphical interface.
- Ubuntu has some of the highest compatibility with existing computers.
- Ubuntu provides easy software update options.
- Ubuntu has a large portion of Linux users, and online support is abundant.
- Ubuntu has fewer driver issues than other systems when adding new hardware.

If you are using ANY version of Linux instead of Microsoft or Apple, you are probably achieving better privacy and security in regard to your digital life. Unlike Apple, Linux does not require an online user account in order to use core services and upgrade applications. Unlike Microsoft, Linux does not demand personal usage data. Unlike both commercial options, Linux is open-source, and the code is vetted by many professionals before each release. If you are interested in achieving extreme privacy, I hope you will consider Linux as your primary computer. The following tutorial will create a new Linux machine with slight modifications for privacy and security.

- Navigate to https://www.ubuntu.com/download/desktop and download the latest Long-Term Support (LTS) Desktop version. At the time of this writing, it was 20.04. This will save a large ISO file to your computer.
- Visit https://tutorials.ubuntu.com/tutorial/tutorial-how-to-verify-ubuntu and verify the download based on your current operating system. This is optional, but important. This will confirm that the version you downloaded has not been intercepted, potentially possessing undesired software. If this sounds unnecessary to you, research the Linux Mint hack of 2016 when this exact scenario happened.
- Create a bootable USB device from the ISO file.
- If on an Apple computer, download Balena Etcher (https://www.balena.io/etcher/), launch the program, select the ISO, select the USB drive, and execute the "Flash" option.

- If on a Windows computer, download Etcher as mentioned above or **Rufus** (https://rufus.akeo.ie), install and launch the program, select your USB device and select the ISO file using the small button in the lower right. Execute the creation.

You should now possess a USB device which is ready to install Ubuntu Linux onto a computer of your choice. If you have an old unused computer collecting dust, that is a great opportunity to try Ubuntu without committing heavily. If you only have your primary machine, you may be able to "dual-boot" both your current operating system and Ubuntu. There are numerous online guides for this. For our purposes, I will assume you are installing Ubuntu as a primary (and only) operating system directly to a machine. I have successfully installed Ubuntu on practically every Windows or Mac machine I have seen. If you are considering purchasing a new machine specifically for Linux, I highly recommend **System76** (system76.com). All of their laptops have the Intel Management Engine disabled. This tiny operating system within the firmware of the processor could potentially allow unrestricted, and unknown, remote access to your machine. There is much debate about the likelihood of this happening, but I welcome the paranoia. I use a System 76 machine as my daily driver. This is NOT a paid endorsement, and I purchased the machine myself (through anonymous payment of course). The following will install Ubuntu Linux to your machine and harden the settings.

- Insert the USB device and power on the computer. If the device is not recognized, research the appropriate option to select a boot device for your computer.
- On the Welcome screen, select your language and choose "Install Ubuntu".
- Choose "Normal Installation" and check both download options under "Other".
- If you no longer need any data on the drive inside your computer, choose "Erase disk and install Ubuntu". This will destroy any data present, please be careful.
- Select both "Encrypt the new…" and "Use LVM…" on this screen.
- Enter a strong password which you can remember and is not in use anywhere else.
- Choose a location in your time zone, provide a generic name such as "Ubuntu Laptop", and select a password. If desired, it could be the same as the password chosen to encrypt the operating system. For ultimate security, it could be different. You will need both passwords upon each boot.
- Click "Install Now" and "Continue". Allow the installation to complete.
- Click "Next" twice on the welcome screen.
- Select "No, don't send system info", "Next", and "Done".
- If you receive a notice about updates, click "Install Now" and allow to reboot.
- Upon reboot, click the nine dots in the lower left, and open Software Updater. Verify the computer is up to date.

You now possess a full Ubuntu Linux installation. Right away, you are very private and secure, but I always make a few modifications before introducing Ubuntu to a client. The first priority is to remove the Amazon Launcher and all traces of Amazon from the machine. Ubuntu receives a kickback when Amazon is used within this operating system, and I do not tolerate that type of forced-tracking. Ubuntu claims they cannot see purchase data, but the software is still unnecessary and invasive.

- Click the nine dots (lower left) to open the applications menu.
- Scroll down to "Terminal" and click it.
- Enter "sudo apt purge ubuntu-web-launchers", and provide password.
- Enter "y" when prompted for confirmation.

This completely removes the Amazon package and provides a small additional layer of privacy.

AntiVirus: This is optional, but an occasional scan for viruses is not a bad thing. Similar to Apple, I install ClamAV, but the directions are substantially simpler.

- Open Terminal and enter "sudo apt install clamav clamav-daemon".
- Confirm installation with "y".

The commands to update and scan are identical to the Apple tutorial.

- sudo freshclam -v
- sudo clamscan -i -r /
- sudo clamscan -i -r --remove=yes /

System Cleaner: Similar to Windows, I recommend BleachBit as my daily system cleaner. Type the following into Terminal to install the application.

- sudo apt install bleachbit

Clicking the nine dots in the lower left will present two BleachBit applications. The second icon executes the software with administrative privileges and is the option I choose. Upon first launch, click "Close" to accept default configuration. Similar to Apple, I select every option except the "Free disk space" feature.

You can customize the Ubuntu interface any way desired. I like to remove unnecessary icons from the favorites bar (left) and add more appropriate options. I also change the wallpaper and screen saver to a solid dark color. Play with these features to find your preferred look. If you desire a program similar to Little Snitch for Linux, you can research Open Snitch. I have

tested this software, but found it unnecessary. Linux does not collect information in the same way Apple does, and most applications I use on Linux do not send data without my knowledge. Your level of paranoia may demand this free application.

You should now have a very stable, and very secure Linux operating system. The entire disk is encrypted, and you possess basic settings which will prevent most online attacks. Using Linux instead of Windows will dramatically decrease the likelihood of a virus impacting your usage. Many clients believe they cannot work in Linux because it does not offer some premium software applications. Some are surprised to discover that the vast majority of their usage is within a web browser, which they find faster in Linux than other options. Regardless of your choice of Mac, Windows, or Linux, you are only as secure as your online habits. Linux is not a silver bullet which allows you to let your guard down while online.

Password Vulnerabilities

In 2018, I had a client that kept getting "hacked". Someone was accessing her email, calendar, and private messages. Changing her password never helped much, and her stalker was showing up any time she had plans with her friends. Her mistake was the use of recycled passwords. She had a single word that she liked to use, and simply added the name of the website after it. If her word was "privacy", her passwords were "privacyfacebook", "privacygmail", and "privacyapple". It was easy for her assailant to access her accounts. He knew the main word in her password because of data breaches.

There are thousands of breached databases floating around online, and you are likely in one or more of them. Searching your own email addresses or usernames on websites such as haveibeenpwned.com may reveal the places you are exposed. However, none of these sites reveal the password. For that, you would need to collect the breaches yourself or pay for one of the premium lookup services. Most popular and known data breaches can be found online easily, including the plain text passwords associated with each.

For our purpose, it will not matter whether you are exposed. Assume that all of your passwords have been compromised. During an initial visit with a client, I determine the important sites which will need to be accessed, and begin the process of changing every password in his or her digital life. This will require a password manager.

This is where I try desperately to avoid a debate about which password manager is best. Simply choosing a side of offline or online managers is likely to get me in trouble quickly. Remember, we want extreme privacy and security. Therefore, all of my clients in immediate danger transition to an offline password manager, specifically KeePassXC.

Password Manager Crash Course

KeePassXC is an open-source password manager that does not synchronize content to the internet. There are many convenient online password managers that are secure and keep all of your devices ready for automated logins. Those are great for entry-level security, and millions of people are safely using them. It is not enough for our needs. Furthermore, I believe that my clients should choose an individual machine for sensitive account access, eliminating the need for synchronization between devices. My clients all receive a tutorial on KeePassXC.

KeePassXC is cross-platform and free. It will work identically on Mac, Windows, or Linux. Download the software from https://keepassxc.org, and conduct the following as an exercise.

- Launch KeePassXC and select Database > New Database.
- Provide a name to your new password database, such as Passwords.
- Move the encryptions settings slider completely to the right and click Continue.
- Assign a secure password which you can remember but is not in use anywhere else.
- Click Done and select a safe location to store the database.
- Close the program and verify you can open the database with your password.

You now have a secure password manager and database ready for use. Assume you are ready to change the password to your email provider. Navigate to the menu which allows change of password for your provider. Next, conduct the following within KeePassXC.

- Right-click within the right column and select New Group.
- Name the group Email and click OK.
- Select the Email group on the left menu.
- In the right panel, right-click and select New Entry.
- Provide the name of your email provider, username, and URL of the site.
- Click the black dice icon to the right of the Repeat field.
- Click the eyeball logo underneath the black dice logo.
- Slide the password length slider to at least 40 characters.
- Copy the generated password and paste into the Password and Repeat fields.
- Change your email password to this selection within your email provider.
- Click OK and save the database.

You successfully created a new, secure, randomly generated password for your email. You will not remember it, but your password manager will. From this moment forward, you will change every password to any site that you access upon logging in. The next time you log in to your secure sites, change the password. Allow your password manager to generate a new random

password containing letters, numbers, and special characters. If the website you are using allows it, choose a password length of at least 50 characters. When you need to log in, you will copy and paste from the password manager. For each site which you change a password, your password manager will generate a new, unique string. This way, WHEN the site you are using gets breached, the password collected will not work anywhere else. There should be only a handful of passwords you memorize, which brings us to the next point.

The password to open your password manager should be unique. It should be something you have never used before. It should also contain letters, numbers, and special characters. It is vital that you never forget this password, as it gives you access to all of the credentials that you do not know. I encourage clients to write it down in a safe place until memorized.

Finally, it is vital to make a backup of your password database. When you created a new database, you chose a name and location for the file. As you update and save this database, make a copy of the file on an encrypted USB drive. I will explain more about this later, but be sure to always have a copy somewhere safe, and not on the internet. If your computer would completely crash, and you lose all of your data, you would also lose all of the new passwords you have created. This would be a huge headache. Prepare for data loss now.

Personally, I keep my KeePassXC database within an encrypted VeraCrypt container within a laptop drive with full-disk encryption. I then backup this entire drive to an external hard drive with full-disk encryption. This external drive is left with a trusted friend who could ship it to me if ever needed. Without knowing the passwords to the encrypted drive, VeraCrypt container, and KeePassXC database (all unique), this drive is useless. These three passwords are the only passwords in my life I keep in my memory.

If you want integrated browser support, KeePassXC has this option. You can install the browser extension into Firefox (addons.mozilla.org/firefox/addon/keepassxc-browser/) or Chrome and easily populate passwords into websites without leaving the browser. I believe this is safe, and that passwords never travel over the internet from the app, but I do not use it. I believe that copying passwords into websites should be a deliberate act that requires effort. I don't want a machine doing this for me. However, many clients insist on having this convenience. Therefore, let's walk through the process.

- Once you have KeePassXC installed, configured, and in possession of your passwords, install the KeePassXC Browser extension into the browser of your choice (I prefer Firefox).
- In the "Preferences" or "Options" of the KeePassXC application, click the "Browser Integration" option in the left menu. Select the "Enable browser integration" option and select your browser.

- Return to your browser and open the KeePassXC Browser menu. Choose to connect to the database, and authorize this connection within the KeePassXC application. Provide a name, such as "Firefox", in order to identify this pairing.
- If desired, select the "Never ask before accessing credentials" option in the Advanced menu of the Browser Integration menu within KeePassXC. This will prevent the application from requiring your authorization for every website you visit.

You should now be able to populate passwords for various websites directly within the browser. Note that the URL field within an entry on KeePassXC must contain the exact address of the login page of the site you are visiting. This will take some tweaking over time, but will eventually provide a seamless experience within the browser. Remember, the benefit of this scenario is that your password database never leaves your computer. It is never stored online anywhere.

The concern I often hear from clients is how they should sync their offline database to their other devices. While you could copy the database and manually sync it to other computers and mobile devices, is that really necessary? My stance is that you should only log in to sensitive accounts from a single trusted computer. My primary laptop possesses my KeePassXC program and database. This is the device I use when I need to log in to an account of any type. I never log in to anything from my phone(s) or other devices and computers. I realize this is limiting, but I also remind you that we are only considering extreme privacy techniques. If you insist on possessing your password database on a mobile device such as an iPhone, I recommend **Strongbox** (https://strongboxsafe.com).

Strongbox is a free iOS application with premium purchase options. The free version allows you to open any KeePassXC database on your mobile device, and copy passwords from it into other applications, such as your browser. There are two big advantages to this scenario. Obviously, you have the convenience of passwords being present on your mobile device. This allows easy login to various apps and websites. Second, it provides a backup in case of corruption on your primary device, such as a laptop. Once you have Strongbox installed on your mobile device, the following steps will copy your database over.

- Connect your iPhone to a laptop with iTunes.
- Launch iTunes and click on the device icon.
- In the left menu, click "File Sharing".
- Select Strongbox in the right window and click the "add" button.
- Select your KeePassXC database and click "Add".
- Close iTunes and disconnect your device.

You can now open Strongbox on your mobile device and access your KeePassXC database. You will need to supply the password to this database each time you open it. You can make this easier by allowing your biometrics options, such as a fingerprint, to automatically log you in, but this is a paid feature. While convenient, it adds more risk. Changes made to your primary database on your laptop will not be applied to this mobile version. You would need to replace the mobile version with a new copy on occasion.

There are numerous customizations you can make within Strongbox. The most important option for my clients is to make the database read-only. This is to ensure that they do not accidentally modify this database and present a conflict between their database on their laptop. They should only make changes on that primary database, and consider the iOS version as a read-only backup. If you want to replicate this, click on the "Database Management" option in the lower left of the KeePassXC database, and enable the "Open as Read-Only" setting.

Again, I want to stress that browser extensions and mobile solutions are optional. In a perfect scenario, you do not need access to your passwords on a mobile device or within automated browser extensions. Only you can decide the balance of security versus convenience which is best for you. If these conveniences are required to ensure you use a password manager for all of your accounts, I believe they are justified. If you can get by without them, even better.

The attraction to online password managers such as Lastpass and Dashlane is the ability to sync the password database to all devices over the internet without manual interaction. I understand the benefits of these features, but it also comes with risk. All reputable online password managers encrypt the passwords locally on the user's device before syncing with their own servers. Theoretically, no one at the password manager company would have the ability to see your individual passwords. However, nothing is hack-proof. It is only a matter of time before something goes wrong.

By keeping your passwords in an offline database such as KeePassXC, you eliminate this entire attack surface. However, I respect that some clients do not want to apply the time and effort of maintaining a secure password database locally. If you insist on using a cloud-based password manager, I highly recommend **Bitwarden** (https://bitwarden.com/).

Bitwarden is open source software with all of their source code free for anyone to review. They have been audited by reputable third-party security auditing firms as well as independent security researchers. While nothing is bullet-proof, I believe this is the most secure option for an internet-based solution. Bitwarden does not store your passwords in plain text. It stores encrypted versions of your passwords that only you can unlock with your master password. Your information is encrypted locally on your device before being sent to their cloud servers. Most of my clients rely on the free version of this product, but advanced users may require a

paid tier. Installing the Bitwarden application on all of your devices simplifies the synchronization of your database. It eliminates the headaches of manual updates.

Creating and storing secure passwords through Bitwarden, or any other online service, should be similar to other password managers, such as KeePassXC. Due to constant user interface updates, I will not present detailed usage instructions. It is vital that you feel comfortable with the application you choose, and that you understand how to update and save any changes.

If you choose to rely on an online password manager, be sure to export all of your data on occasion. If the service should shut down, terminate your account, or experience data corruption, you might find yourself in a bad situation. If using Bitwarden, the following steps will download an offline copy of your passwords.

- Log in to your web vault at https://vault.bitwarden.com.
- Click "Tools" in the top navigation bar.
- Click "Export Vault" under the side navigation.
- Choose a file format, type in your master password, and click "Export Vault".

I recommend placing your backup within your VeraCrypt protected container. In the worst-case scenario, you could import this backup into another password manager solution and have the ability to access all of your accounts. I have had three clients who lost access to their passwords through their online password managers and had to attempt password resets through every account. A backup would have prevented this frustration.

Again, I do not use cloud-based password managers, and I encourage my clients to avoid them, but I respect those who require this level of convenience. ANY reputable password manager is better than none at all. Regardless of the password manager route you choose, you want to slowly change all of the passwords you use to unique, random replacements. This does not need to be done overnight, but I encourage you to start with the most important accounts such as your primary email addresses and any online calendars.

Make sure you are using a trusted device, such as your new laptop, while making these changes. If you change all of your passwords from your old Windows machine which possesses a keylogger or other malicious software, you could be sending your changes to an adversary. Also, make sure you are on a secure network. Never change passwords while on public Wi-Fi. In a moment, you are going to be switching to new accounts, but it is vital to protect any of the old accounts before moving on.

Two Factor Authentication (2FA) Crash Course

You are likely already using some form of 2FA without asking for it. Have you ever logged in to a financial institution website and then be told to check your email for a code? That is 2FA. It is something you know (such as a password), and something you have (such as access to your email address or cell phone number). It is vital to enable 2FA anywhere possible. This includes banks, email accounts, social networks, credit card companies, and sometimes software applications. 2FA is mostly associated with receiving a six-digit temporary code via text message any time you need to log in to an online service. This is actually the least desired method. My preferences, in order, are the following.

Hardware Token: I use a **Yubikey** (yubico.com) daily. This small device which plugs into my USB port is required before I can access my business email and other sensitive accounts. When I log in to a website set up for 2FA through Yubikey, the site waits until I touch my finger to the device, which sends a one-time code to the service. The online site confirms the correct Yubikey was used and provides me access to the service. Without the presence of this physical USB device, I cannot gain access to my accounts. The configuration instructions for adding a Yubikey to any online service varies, but you should find instructions on the appropriate websites for each service.

Software Token: If a service does not support a hardware token, then I prefer using **Authy** (authy.com) as my software-based 2FA. I choose Authy over open-source options simply because it is easier on my clients. I have learned that making anything overly complicated will result in lack of use. I do believe that options such as FreeOTP are possibly more private, but they are more difficult to use on multiple devices. Authy works on macOS, Windows, iOS, and Android, and you can use a temporary code from any device at any time. The following explains my method of configuring Authy for a client.

- Download the Authy application to both the new laptop and new iPhone.
- Through the iOS app, create a new account with the Authy service.
- Under Devices (lower right) enable Allow Multi-Device.
- Open the desktop Authy app and follow instructions to connect to an account.
- Once you successfully have Authy working on both devices, disable Multi-Device.

You can now add any services you use which allow a software-based 2FA. When configured properly, you will log in to a service and it will prompt you for a six-digit code. Opening Authy on either device will present a new code every thirty seconds. Entering that code completes the login process. You will likely find the necessary instructions within the security options of each service. You can also visit authy.com/guides for details about the most popular services.

SMS Token: If an online service you use only supports 2FA via a text message, it should still be used. While not optimal, it is better than no protection at all. I never recommend using your cellular number provided by your carrier, as it is prone to SIM swapping attacks. Instead, I use Google Voice. This may seem surprising due to my criticism of Google's privacy policies, but their security is top-notch. Their Google Voice service is free and can be protected by a hardware token, such as a Yubikey.

- Create a Google account or preferably use an account already active.
- Navigate to google.com/voice and request a new number (if you do not have one).
- When prompted, provide a landline number for verification, such as an office number.

This will provide you unlimited use of a new virtual telephone number. You can provide this new Google Voice number whenever prompted for a 2FA option within an online service. Be sure to secure the Google account with a hardware or software token, preferably a Yubikey. If you set up your phone as mentioned previously, the codes will be sent to your email as you request them. Some readers of the previous edition of this book expressed concern over the ability of companies to track us through use of a single hardware token (Yubikey) across multiple accounts. This is a valid concern if you are using the One Time Password (OTP) option of Yubikey, but not a big concern if using the more secure Universal 2nd Factor (U2F) option. I will explain each.

OTP provides a unique code every time you touch your Yubikey. You can test this while within a text processing application. Every time you activate the Yubikey, a new line of data is entered. However, the first 12 characters are always the same and represent the serial number of the Yubikey. This is concerning, as it could associate two accounts with the same device; therefore, associating multiple accounts to the same individual (you). It could also leak your Yubikey serial number upon accidental touch during a text conversation or make you slightly more prone to a phishing attack when someone attempts to steal a valid token in order to access your account. However, most sites do not use OTP today. If they do, they also offer a U2F option.

U2F creates a unique challenge and response each time it is configured for an account. There is no static line of text which can be misused. Google, Twitter, and others offer hardware token service through U2F only. Therefore, using the same Yubikey within multiple Google accounts does not clearly connect them to each other. Always look for a U2F option when registering a Yubikey with a service. If no clear protocol is identified, do your research.

The bottom line is that ANY 2FA is better than NO 2FA. Practically every "hacking" scenario which happens to a client could have been prevented by using 2FA. Hardcore privacy and security enthusiasts should look into the OnlyKey, which is explained toward the end of the book. While I use one, I have yet to have a client commit.

Encrypted Storage & Backup Crash Course

I mentioned encryption earlier, and it has been a popular hype word over the past few years. Encryption can mean many things, depending on how it is applied. Previously, we applied full-disk encryption to the entire drive of the computer. In this section, it refers to software encryption on a physical device, such as a USB drive. This works by automatically converting data on a drive into a form that cannot be understood by anyone who doesn't have the password to reverse the conversion. Without the proper password, the data remains inaccessible. This is extremely important in case you lose a device, especially a portable drive used as a backup. If I steal your USB device, and you did not apply encryption, I can access all of your files without the password to log in. If you encrypted your data, I cannot extract anything. I apply the following backup and encryption practices for the removable devices for each client.

I first choose a backup device appropriate for the situation. For most clients, I choose a SanDisk Ultra Fit USB drive. These can be easily found in 16GB, 32GB, 64GB, and 128GB options, and I choose the largest possible. These are small and reliable. If my client only needs to access this device on an Apple computer, then I apply FileVault encryption to the USB device as explained previously. If my client needs access to this drive on a non-Apple device, I create an encrypted container through VeraCrypt by conducting the following.

- Click "Volumes" > "Create New Volume" > "Create an Encrypted File Container".
- Choose "Standard VeraCrypt volume".
- Click "Select File", choose a name such as "Backup", and select your USB device.
- Click "Save" > "Next" > "Next".
- Enter the volume size lower than the specified limit (round down to nearest number).
- Choose a strong password for this container and click "Next" > "Next" > "Next".
- Move your cursor randomly as the pool completes. When finished, click "Format".

You now possess an encrypted container on a USB device. You can store anything within this container once it is mounted. To do this, open VeraCrypt, click Select File, choose the "Backup" file on the USB, select Mount, enter the password, and you should see that container as a new drive on your computer. Now that the device possesses an encrypted container ready for storage, we need to establish a backup solution. I prefer an open source solution rather than proprietary offerings from Apple or Microsoft. For my clients, I recommend **Free File Sync** (freefilesync.org). This site possesses free tutorial videos which demonstrate usage better than I can explain in a couple of paragraphs. Always understand your backup solution before relying on it.

The vital lesson here is that you should have a backup strategy which involves encrypted data. Backup anything important often, and only backup to an encrypted drive. If, or more likely when, this USB device is lost or stolen, you will not panic. The content can never be visible without your password. If your primary computer suffers a hard drive crash, you have a backup to restore the data. I am a bit extreme on my own backup solution, and whenever I have a highly-targeted client, which I will explain next.

First, my computer possesses full-disk encryption. Within that drive, I possess a VeraCrypt encrypted container 128GB in size. Within that container is everything important to me including photos, videos, documents, business data, and even my password manager. You must know the computer password and the VeraCrypt password to see anything. I possess a 128GB USB drive with full-disk encryption. It then contains a 127GB VeraCrypt container. I use Free File Sync to occasionally backup the content of the container on my computer to the content of the container on my USB drive. I then replicate this process with an additional external media which is stored off-site in case of true emergency. Is this overkill? Maybe. I would rather be safe than sorry. My clients store sensitive information which would be very valuable in the wrong hands. I take every precaution I can.

In 2019, I was forced to test my encryption and backup strategy during a series of unfortunate events. I had recently updated my password manager, KeePassXC. This new version possessed a bug in the code which would delete the database if stored on a Mac computer but inside another operating system file structure. Since my KeePassXC database was stored within a VeraCrypt container on my MacBook Pro, I was part of a small minority of users who experienced this flaw (this problem was patched a few days later by KeePassXC). When I closed KeePassXC, the database was completely deleted without any possibility of recovery. There was no warning, and I was unaware of the issue. When I conducted a daily backup of all data to my USB drive, it removed the copy of the KeePassXC database on it and replaced it with an empty folder. I now had absolutely no copy of my KeePassXC database, which was a catastrophe. When I opened my password manager, there was no option to see my passwords. After a brief moment of panic, I reached out to a friend who could help.

In my previous example of how I store my data, I mentioned an off-site external media which possessed a duplicate copy of all vital data. This is in the form of a 1GB micro SD card which contains a single 1GB VeraCrypt container. The password to open this container is unique from anything else, and I have it memorized. Without this password, the data is useless to anyone who takes possession of the card. This card was placed inside of a "hollow nickel" and stored secretively inside the home of a friend and former colleague. This is a real U.S. nickel which is made from two unique coins. Each coin is die-cut in order to create a top piece (heads) which fits into the bottom piece (tails) and allows for a hollow space in between, large enough to store a micro SD card, as seen on the next page in Figure 3.02. These cost approximately $20-$25 online.

Figure 3.02: A hollow nickel with a micro SD card stored inside.

I called my friend and told him I was in a serious situation, and I needed his help without asking many questions. This person works in the intelligence community, so the request was well-received. I advised him to go into his upstairs bathroom and remove the power receptacle cover next to the mirror. He would then notice a nickel resting on the bottom of the outlet box within the wall. Remove that nickel and tap the edge of it on the bathroom sink. The top of the nickel will come loose and can be removed, revealing an SD card. The SD card should be inserted into a computer and the 1GB file should be uploaded to my own web server in a specific directory.

My friend agreed and completed each step. I then asked him to place everything back where it was, and that I would explain everything more over a beer the next time I was in town. Whenever I visit my friend's home, I update the contents of this drive without anyone's knowledge. It is much smaller than my other backup, but only contains the absolutely necessary data I would need in case of an emergency. This includes a current copy of my password manager, client documents, business files, and scanned copies of any identification I may need while abroad. I chose this friend carefully, as I know he is home often, he is extremely trustworthy, and he respects my extreme privacy antics. Hopefully you have someone similar in your life.

After he uploaded the 1GB VeraCrypt file, I was able to open it and destroy the online copy. I then had access to my password manager and could now access my passwords. This version of the database had not been updated in a few months, so I was still missing some recently changed passwords, but my email archive identified those accounts quickly. I was relieved to have my accounts back, as many of them date back over ten years.

I hope this serves as a reminder to the importance of an offline backup away from your home. If I ever find myself overseas with a lost passport, my friend can give me the data I need to obtain a new copy. If my hotel is burglarized and all of my data is stolen, my friend can get the essentials to me. I also maintain a hollow nickel near my home which contains a 128GB card with a full backup of all data. It takes me at least 20 minutes to retrieve it from my property. If someone can find my home, locate this nickel, open it to reveal the card, and beat the encryption, I deserve to be hacked.

Private Web Browser Crash Course

Before we consider connecting to various websites in order to harden our accounts, we should configure a secure web browser. I recommend, and solely use, the Firefox web browser at all times. Your new Apple computer has its own browser called Safari, but I rarely touch it. Windows possesses Microsoft Edge, which I have not opened in several years. The only time I would consider using these options is to connect to https://www.mozilla.org/firefox and download Firefox. Once Firefox is installed and configured, I hide any references to Edge or Safari on my clients' machines. Installation of Firefox is easy and guided, and you can accept all default options. Once installed, execute the application and consider the following modifications.

- Click on the menu in the upper right and select "Options" (Windows) or "Preferences" (macOS).
- In the General options, uncheck "Recommend extensions as you browse" and "Recommend features as you browse". This prevents some internet usage information from being sent to Firefox.
- In the Home options, change "Homepage and new windows" and "New tabs" to "Blank page". This prevents Firefox from loading their own site or services in new pages and tabs.
- In the Search options, change the default search engine to DuckDuckGo and uncheck the "Provide search suggestions" box. This prevents queries from going directly to Google, and blocks the Google API from offering search suggestions.
- In the Privacy & Security options, select the "Strict" option under Content Blocking.
- Check the box titled "Delete cookies and site data when Firefox is closed".
- Uncheck the box titled "Ask to save logins and passwords for websites".
- Change the History setting to "Firefox will use custom settings for history".
- Uncheck the boxes "Remember browsing and download history" and "Remember search and form history".
- Check the box titled "Clear history when Firefox closes". Do not check the box titled "Always use private browsing mode", as this will break Firefox Containers.
- Uncheck "Browsing history" from the "Address Bar" menu.
- In the Permissions menu, click "Settings" next to Location, Camera, Microphone, and Notifications. Check the box titled "Block new requests…" on each of these options.
- Uncheck all options under "Firefox Data Collection and Use".
- Uncheck all options under "Deceptive Content and Dangerous Software Protection". This will prevent Firefox from sharing potential malicious site visits with third-party services. This leaves you more exposed to undesired software attacks, but protects your internet history.

Firefox allows users to modify many configuration settings, and some of these deal with privacy and security concerns. Though some of these changes can be made in the menu of Firefox's preferences, changes made through about:config tend to be more durable and granular. To access the list of configuration settings, open Firefox and type "about:config" into the URL bar. You will receive a warning about making changes within this area, but the modifications we make will be safe. Choose to accept the risks. Some of these about:config settings may already be on the "correct" setting, but most probably will not. To change most of these settings you can simply double-click the setting to toggle it between "True" and "False". Some may require additional input, such as a number. Because the list of about:config settings contains hundreds of entries, you will probably wish to search for all of these through the search bar in the about:config interface.

- geo.enabled: FALSE: This disables Firefox from sharing your location.
- browser.safebrowsing.phishing.enabled: FALSE: This setting disables Google's "Safe Browsing" and phishing protection. If this setting is "true" Google will be able to scan (and store) the sites that you visit for the presence of malware.
- browser.safebrowsing.malware.enabled: FALSE: Again, this disables Google's ability to monitor your web traffic for malware, storing the sites you visit.
- media.navigator.enabled: FALSE: Website operators will identify your computer as unique to enable tracking around the web. One such tactic is to track the status of your webcam and microphone (ON/OFF). This disables the ability for website operators to see this information.
- dom.battery.enabled: FALSE: Another technique used by website operators to track you is to view your exact battery levels. This setting blocks this information.
- extensions.pocket.enabled: FALSE: This disables the proprietary Pocket service.
- network.trr.mode: Change from 0 to 2. This will be used for encrypted DNS.
- network.security.esni.enabled: Change from False to True, also for encrypted DNS.

WebRTC: These settings address a potential vulnerability of leaked IP addresses.

- media.peerconnection.enabled: FALSE
- media.peerconnection.turn.disable: TRUE
- media.peerconnection.use_document_iceservers: FALSE
- media.peerconnection.video.enabled: FALSE

It is not vital that all of these security settings be applied to your systems. Firefox natively respects your privacy and security more than other browsers. These recommendations are for those that want to tweak additional settings that may provide a layer of protection, even if minimal. Next, I will discuss the abundance of helpful browser extensions called add-ons.

In the previous edition of my (now outdated) book *Hiding from the Internet*, I recommended NoScript as the ad-blocker of choice. Not only does NoScript block ads, it also blocks any other type of script that is attempting to run on the page. This helps prevent tracking, malicious code execution, location sharing, and a number of other processes that could undermine your privacy and security. However, NoScript comes with its own problem, which is that it is notoriously difficult to use. I have found a simpler alternative called **uBlock Origin**. uBlock Origin is completely free and open source. It blocks a number of tracking behaviors and security vulnerabilities. It is highly customizable, while remaining relatively easy to work with. uBlock Origin works from blacklists which block trackers specified in the list(s). The add-on comes with several lists enabled, but there are several more that can be added through simple checkboxes in the preferences. Keep in mind that the more blacklists you enable, it may be more difficult to work with the browser. This section may seem a bit overwhelming but experimenting with the advanced settings should help you understand the functionality. Let's start with the basics.

Install uBlock Origin from the Firefox add-ons page or directly by navigating to the application's website at https://addons.mozilla.org/en-US/firefox/addon/ublock-origin/. You are now protected on a basic level. By default, most known invasive advertisements, tracking code, and malicious content is blocked. This step alone would provide much needed protection from the internet. However, we can take it a step further.

Click on the uBlock Origin icon in the menu and select the Dashboard icon to the right. This will open a new tab with the program's configuration page. On the Settings tab, click the option of "I am an advanced user". Click on the Filter lists tab and consider enabling additional data sets that will protect your computer. I select all options within the Ads, Privacy, Malware Domains, and Annoyances categories. After you have made your selection, click the Update Now button at the top of the page. This will refresh all of the data and apply your new settings. You now have extended protection that will be applied to all visited websites without any interaction from you. When you encounter a web page with a lot of advertisements, such as a news media website, it should load much faster. It will block many of the pop-ups and auto-play media that can be quite annoying when conducting research. This protection will suffice for most users, but dedicated privacy enthusiasts may choose to take a more advanced approach.

After you have enabled the Advanced settings as explained above, clicking on the uBlock Origin icon should now present an expanded menu which will change as you visit different sites. In order to explain the function of this menu, I will conduct a demonstration using the website cnn.com. Scrolling down this list of scripts that have either been loaded or blocked, you can see several questionable scripts such as Facebook, Sharethrough, and Turner. These scripts allow tracking across multiple websites and are the technology responsible for monitoring your interests, web history, and shopping habits.

This menu is split into three columns. The first simply identifies the type of code or domain name of the script. The second column is global settings. Anything changed here will apply to all website visits. The third column contains settings for the current website. A single plus sign (+) indicates that less than ten scripts were allowed from that specific option. Two plus signs indicate that between ten and one hundred scripts were allowed. The single minus sign (-) indicates that between one and nine scripts were blocked from that domain, while the dual minus signs tell us that ten to one hundred scripts were blocked. This is all default behavior and provides a balance of functionality and security. uBlock Origin decides which content should be allowed and which should be blocked.

Using this same page, let's modify the options. Click on the far-right portion of the first cell in the third column. This turned the entire third column red in color. This action activated an option to refresh the page (middle arrows) and an option to save the change (upper left "padlock"). Since I blocked every script, the page would not fully execute. It could not load images, design scripts, or any JavaScript. This is not useful at all, so I disabled my actions by clicking on the middle section of the top cell in the third column, which turned the entire column back to grey in color. Saving these changes and refreshing the page brought me back to the original site.

We can also take this to the opposite extreme. Click on the far-left portion of the top cell in the third column. This turns the entire column green in color, and allows all scripts to load on cnn.com. This includes the dozens of intrusive scripts that could load advertisements on the page. You can also see that small plus signs confirm that scripts were allowed to run while the minus signs state the opposite. For most users, this allowance would seem irresponsible.

Next, we will modify the second (middle) column, which will apply the settings globally. By default, all options are grey in color. This indicates that the default block list is applicable, and only invasive scripts will be blocked everywhere. Click on the far-right portion of the top cell in the second column. This turns the entire column red, and indicates that all scripts across all websites will be blocked. After saving changes, every website will only load the most basic text content.

Loading a page such as a Twitter profile results in no usable content. By clicking on the uBlock Origin icon and clicking the middle sections of specific cells within the third column, you can enable those scripts without allowing everything on the page. In this example, the entire second column is red. This indicates that all scripts are blocked globally. The third column is mostly red, but the options for twitter.com, twimg.com, and others are grey. Those scripts will be allowed, if approved by uBlock Origin's rules, only for that domain. If you loaded a blog that has scripts from Twitter, they would still be ignored.

These are extreme examples. Let's bring this back to some sanity. The following is how I recommend using uBlock Origin. Install, enable advanced options, and proceed with your work. When you arrive at a website that is blocking something you want to see, open the menu, and click on the far-left section of the top cell in the third column. That will allow everything to load on that page, and that page only. When you are about to navigate to a questionable site that may try to install malicious code on your machine, click on the far-right section of the top cell in the second column. That will block all scripts on all pages. Conduct your internet usage and reverse the change when you are finished. Remember to click the save button (padlock) after each change.

I also use this plugin to bypass website restrictions. As an example, consider my local newspaper, The Chicago Tribune. When you navigate to chicagotribune.com, you are allowed to view three articles before being blocked with a message which states "You've reached your monthly free article limit. To continue reading, subscribe now". Clicking any further articles blocks your access. You may have seen similar messages from websites when using any type of ad blocker. Clicking the uBlock Origin icon reveals it is blocking 14 scripts, but something is still running in order to know the number of articles I have read. Choosing the far-right option (red) within the line titled "Inline scripts" blocks these types of annoyances from this domain. Clicking the lock (save) option and reloading the page eliminates the barrier permanently. It also makes the page load much faster. I can now browse this website with unlimited access.

Hopefully, you are practicing these settings and learning how this program functions. It is an amazing option that has protected me many times. If you are doing things right, you have likely completely messed-up your settings and are now blocking things you want while allowing things you do not. Don't worry, we can reverse all of our mistakes by first making the global (second column) settings back to grey (middle section of top cell). Next, return to the dashboard settings of the add-on, and click on the My Rules tab. In the second column (Temporary Rules), click Edit, highlight all of your customizations, and delete them. Click the Save button in this same column and then the Commit button to apply these settings everywhere.

The huge benefit of uBlock Origin over other options is the simple ability to block malicious scripts without customization, while having an option to allow or block any or all scripts at our disposal. This is a rarity in these types of add-ons. The images in Figure 3.03 display these options with scripts allowed (left) and disabled (right).

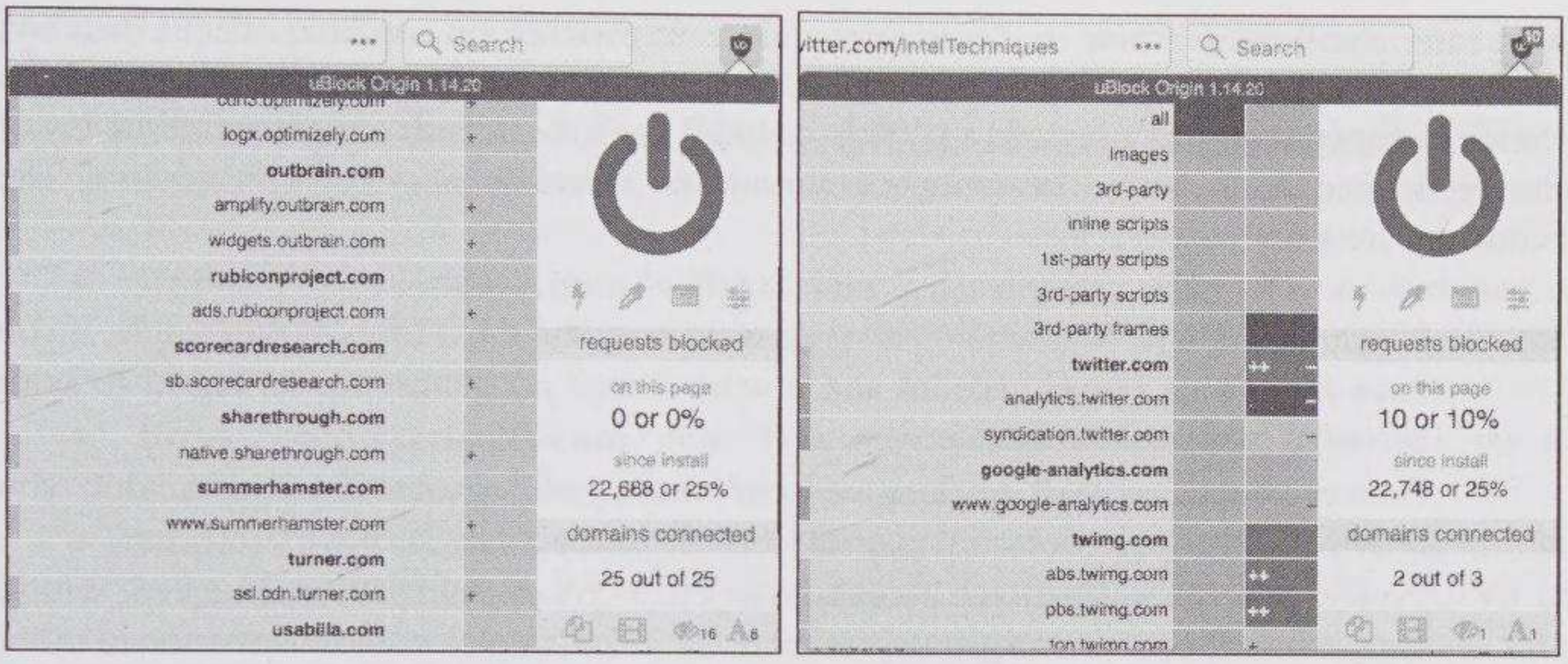


Figure 3.03: Menus of uBlock Origin.

The next Firefox add-on which I use daily is the Multi-Account Containers option from Mozilla. It can be found at addons.mozilla.org/firefox/addon/multi-account-containers. Multi-Account Containers allows you to separate your various types of browsing without needing to clear your history, log in and out, or use multiple browsers. These container tabs are like normal tabs except that the sites you visit will have access to a separate slice of the browser's storage. This means your site preferences, logged-in sessions, and advertising tracking data will not carry over to the new container. Likewise, any browsing you do within the new container will not affect your logged in sessions, or tracking data of your other containers. Below is an example.

I have a container tab open which I use to log in to my email provider. I have my inbox open in this tab. I want to order a product from Amazon, but I do not want them to see any cookies stored by my email provider. I also want to conduct a Google search, but do not want Google to see any data present from my Amazon search. I simply open a unique container tab for each of these events. Each sees the session as unique, and no data is shared from one service to another.

Once installed, you will see a new icon in the upper right which appears as three squares. Click on it and select the container you want to open. Default options include choices such as Personal and Shopping, but you can modify these any way you desire. I have over twenty containers titled Private01, Private02, etc., as well as options titled Email, Amazon, and Banking. You can create, delete, and edit containers from the Containers menu. When you click the Edit Containers or the + buttons, you can change the color or icon associated with a container or change the container name.

You can open links in a new or different container. Right-click on any link, select Open link in New Container Tab, and then select the desired container tab. The new tab will open within the same container as the previous tab. This includes both the default container and in any of the predefined containers. There are many ways to take advantage of this add-on. The following are a few suggestions.

- Log in to multiple accounts on a single website at the same time. For example, if you have a personal Gmail account and a work Gmail account, you can log in to both accounts in separate containers.
- Protect yourself against tracking without needing to log out of websites while you browse. Websites in one container can't track your activity in other containers.
- Protect yourself against web security attacks. Any harmful clicks will be kept within that website's container, so attackers won't be able to hijack your information in other containers.
- Assign a website to a container, so that a specific website will always open in a specific container. I use this for Facebook. If I ever visit Facebook as part of an investigation, the site will open in a new container tab which I designated Facebook. This is regardless of which tab I try to use.

The final Firefox add-on I recommend is **Decentraleyes** (https://decentraleyes.org), which complements uBlock Origin. Websites have increasingly begun to rely on large third parties for content delivery, such as tracking software supplied by Google, Microsoft and various content delivery networks. Blocking this specific code which tracks your activity can often break the website you are visiting. Decentraleyes provides local files to replace the otherwise necessary content in order to improve online privacy. An example should help explain.

When I connect to riverfronttimes.com, the site requires some code called JQuery. This site loads JQuery from Google's servers, and Google collects usage data about my activity on this site. If I block the request to download JQuery from Google, the site will not load properly. The JQuery code is simply required for this site (and many others). With Decentraleyes installed, it intercepts the request to download JQuery from Google and provides a locally stored option instead. The JQuery code is loaded from the browser extension without the need to involve Google. The site loads properly, and Google does not track me with this download. Decentraleyes does not require any configuration. It starts working the moment it is installed.

Some readers may be frustrated with my setup for Firefox and may insist on using a Chromium-based browser. I completely respect this, and offer the option of Brave Browser. Brave is based on Chromium, which is the bones of the Google Chrome browser. Brave insists they have removed all calls to Google which Chromium makes by default, including the use of Quad9 as the DNS provider (instead of Google). If you NEED a Chrome-like browser, I

recommend Brave. If you can use Firefox, I find it to be much more privacy-focused. Regardless of your chosen web browser, you should test your configuration for any potential leaks. I rely heavily on the free service **Browser Leaks** at https://browserleaks.com. There are numerous options within this site, and I outline my favorite below.

- **https://browserleaks.com/webrtc**: This page displays whether your browser is blocking WebRTC IP leaks as previously mentioned. The goal is to receive all red "False" responses.
- **https://browserleaks.com/geo**: This page identifies whether your browser is sharing location data. The optimal response is a red "Denied" result.
- **https://browserleaks.com/proxy**: This page discloses any unique filtering within your network which could make you a more unique visitor to a site. The goal is to receive all red "not detected" results, unless you approve of the technology filter. You may see uBlock filters, which eliminate specific data from entering your session.
- **https://browserleaks.com/social**: This page displays any social networks or online marketplaces which place a login cookie on your machine. As an example, if you are logged in to an Amazon account, you should see evidence of that here. This is a good test to ensure your Firefox containers are functioning properly.
- **https://browserleaks.com/javascript**: This page displays the information available about your connection to any site you visit. Interesting areas include local time, browser identifiers, and operating system data.
- **https://browserleaks.com/flash**: This page displays whether the Flash plugin is installed. My preference is that it is never used.
- **https://browserleaks.com/silverlight**: This page displays whether the Silverlight plugin is installed. My preference is that it is never used.
- **https://browserleaks.com/java**: This page displays whether the Java plugin is installed. My preference is that it is never used.
- **https://browserleaks.com/donottrack**: This page displays your "Do Not Track" browser settings.

Again, this is not a comprehensive list of digital security best practices for various operating systems. This is the bare minimum recommendations in order to continue your journey through extreme privacy strategies. My scope here is to disappear completely and possess better privacy. My own education on digital privacy and security is never-ending. I learn a new or better way to execute my own strategies monthly. Toward the end of this book, I present an entire chapter on obtaining an "Advanced" private digital life. It introduces virtual machines, portable secure operating systems, Do-It-Yourself VOIP solutions, custom Android builds without Google services, and various hardware devices which elevate our privacy and security demands.

DNS Crash Course

I briefly mentioned two specific Firefox settings related to Domain Name System (DNS) queries, but we should have a more detailed conversation about this service. In the simplest explanation, DNS translates domain names, such as inteltechniques.com, into IP addresses in order to locate the appropriate content. In a typical home setup, your internet service provider (ISP) conducts your DNS queries. In other words, your ISP knows every website you visit, regardless of SSL encryption, and knows your billing address. If you did not purchase internet service anonymously, then they also know YOU. ISPs collect a lot of valuable information about you this way, and often sell these details to third parties for marketing purposes. I want to stop that. Whether you use no VPN whatsoever (poor), rely on an application-based VPN directly on a computer (better), or execute a full home firewall as explained later (best), you should modify your DNS settings.

If you are on an Apple machine, enter your "System Preferences", open the "Network" option, select the connection (such as Wi-Fi), click "Advanced", and then "DNS". In the left pane, remove any entries and add 1.1.1.1 and 1.0.0.1. Click "OK" to save. If you are on a Windows 10 machine, open "Settings", then "Network & Internet", then "Change Adapter Options". Right-click your connection and choose "Properties". Click on "Internet Protocol Version 4" and click "Properties". Select "Use the following DNS server addresses" and enter 1.1.1.1 and 1.0.0.1. Click "OK" and repeat for "Internet Protocol Version 6". Your machine should now use the Cloudflare DNS service. As discussed later in the Home Firewall chapter, I recommend this service due to speed, stability, encrypted options, no-logging policy, and third-party auditing through KPMG.

There are a few caveats here. If you are using a VPN application on the computer, it will likely ignore your DNS choices and use its own server. This is acceptable for most. If your VPN crashes, you would fall back to Cloudflare for DNS, which provides better protection than being exposed to your ISP. If you are connected to a home firewall, this is redundant, but not harmful. This prevents SOME snooping from your ISP.

We must now ensure that the connections are encrypted. If you applied the Firefox settings explained previously, you are ready to test your new configuration. The current version of Firefox should offer encrypted DNS by default, but I left the custom settings in the book to ensure we were protected. Navigate to https://www.cloudflare.com/ssl/encrypted-sni/ and conduct a test. You should see green checkmarks next to each of the four tests. If you do, you are hiding much of your internet traffic from your ISP and your VPN. I conduct this test monthly from all of my devices.

VPN Crash Course (Desktop)

I mentioned the importance of a VPN in the previous chapter in regard to your mobile device. This also applies to any computer you use. The same service you selected for your phone should provide an app for your computer. Most reliable VPN providers grant you multiple consecutive device usage. Therefore, you can use the same account credentials on your laptop which you use on your mobile devices. Even if you choose to replicate the home firewall with constant VPN, as explained later, you should still possess a VPN application on your laptop for travel usage. When traveling, I rely on a VPN application any time I am connected to the internet. This is especially important if using any type of public Wi-Fi. Similar to the previous chapter, I rely on ProtonVPN as my provider for my laptop(s). Let's walk through the three levels of VPN options as we did previously for mobile device usage.

Basic: For most readers, and almost every client I have consulted, I recommend sticking with the standard desktop application provided by a VPN company. Whether this is a larger provider such as PIA and ProtonVPN, or a smaller supplier such as Mullvad, the apps provided directly from the company should suffice for your needs. These can be downloaded from the provider's websites. Once installed, simply provide your account credentials and launch your VPN connection.

Intermediate: Similar to the previous chapter, the OpenVPN application is available for Windows and Linux users. Currently, there is not an official OpenVPN application for Mac, but the free app Tunnelblick replicates this protocol. Configuration will require some research, but most VPN companies provide explicit instructions for this option. This allows you to configure your VPN without downloading any closed-source software from the provider.

Advanced: Mac, Windows, and Linux users can manually configure a VPN within their operating systems. However, you may be limited with the protocols available. While I like this option for iOS users, I do not encourage clients to rely on an IPSec protocol within a desktop operating system. If you do not want to download a proprietary VPN application offered by your service provider, I encourage you to research the OpenVPN option above. I believe the "Basic" option is suitable for most readers, especially if you plan to establish the home firewall explained later.

Relying on a VPN company is difficult. We place a lot of trust into the provider(s) we choose, without knowing much about the company or their financial backing. As stated previously, I had recommended PIA for many years. Their merger with Kape Technologies has urged me to slightly step away from this endorsement. Kape, previously known as Crossrider, has been heavily focused on advertising and data collection in the past. Access to millions of privacy-minded VPN users' computers could be a goldmine to them. Therefore, I no longer install

the PIA application on my devices and only recommend their services within a firewall as explained later.

I believe all VPNs are flawed, but still a requirement for us. Almost every VPN provider relies on rented servers across the globe which are out of their control. Many providers unknowingly use the same servers as their competition. A VPN is simply a single layer of protection. Always purchase your subscription anonymously, and I present multiple options for this later. When using a VPN, you are simply placing your internet history into someone else's hands. This sounds bad on the surface, but it is better than doing nothing at all. Without a VPN, we know our ISPs are monitoring, collecting, and sharing our internet activity. With a VPN, we are told that this information is not logged or shared. Are we bullet-proof? No. However, I would rather make the attempt to hide my traffic than do nothing at all.

Some may question the amount of data shared about your online history when you send all of your traffic through a VPN versus your ISP. There are always vulnerabilities which could expose more data than intended, but we can discuss a few misconceptions about your internet traffic. First, we should tackle SSL/TLS. SSL (Secure Sockets Layer) and its successor, TLS (Transport Layer Security), are protocols for establishing authenticated and encrypted links between networked computers. This is related to the lock icon you see in your browser when on any website which begins with "https". This indicates a secure connection, but what does that really mean? I will simplify with a couple of examples.

Assume you are on your home computer connected directly to your internet service provider (ISP). You are not using a VPN. You connect to Google and conduct a search for "inteltechniques". The response URL presented to you, including the search results from the query, is https://www.google.com/search?q=inteltechniques. Does your ISP know you conducted a search on Google? Yes. Do they know you searched for "inteltechniques"? No. This is because Google encrypts the actual search URL. The provider of your internet connectivity can only see the domain name being accessed. It cannot see any details about specific pages or any credentials entered. This is why https versions of websites are so important. Your browser can see this entire URL, but it does not directly share any details with your provider. Now, let's introduce a VPN.

After connecting to your VPN, such as ProtonVPN, you conduct the same search. Does your ISP know you conducted a search on Google? No. Does your VPN provider know you conducted a search on Google? Yes. Does your VPN provider know you searched for "inteltechniques"? No. Why does this matter?

Everyone has a unique threat model, but I will present a few scenarios where you may be concerned. First, consider that I am suing you civilly, and I have convinced a judge to grant me a court order to collect your internet activity. Since I know where you live, I can assume

the provider of your internet service. A court order is issued to your ISP for your internet activity. If your ISP logs your traffic, which most do, the response would tell me every domain which you visited and the dates and times of occurrence. I could use this to prove you were visiting specific websites or transmitting large amounts of data to designated services. If you had a VPN enabled, I could only prove your device(s) were connected through a VPN. I would not know any domains from your activity. A second court order to the VPN provider would not reveal this data. Reputable VPNs do not log this traffic, and IP addresses are shared between thousands of users.

Next, assume I want to know where you live. I know your email provider is Gmail, and a subpoena to them would reveal your IP address at a specific date and time. If this IP address belongs to your internet service provider, a second subpoena will disclose the address of service (your home). If the IP address belongs to your VPN provider, it will not disclose any details about you or the VPN account. A subpoena to the VPN for information about the IP address will reveal no logs and an education about IP address sharing between thousands of strangers.

Now, let's combine the strategies mentioned previously to thwart this behavior. Since you are always connected to a VPN, your ISP knows nothing about your internet traffic. A subpoena to them would not reveal the sites you visit. Since ProtonMail does not log your IP addresses in clear text, they cannot determine your true IP address. Since ProtonVPN and ProtonMail are Swiss-based companies, they would not respond to a subpoena from the U.S. If you purchased a VPN service without providing your name, there is nothing to glean from the VPN provider about your account (such as a personal credit card number or home address). I hope that you now see that all of these strategies strengthen each other.

What do I do? At home, my entire network is behind a fail-proof VPN. I will explain each detail in a later chapter. I do not need individual VPN applications running on my devices while at home. While traveling, I have the ProtonVPN desktop application ready on my laptops. As mentioned previously, I have ProtonVPN servers manually configured on my iPhone.

Many readers may be tired of my promotion of ProtonVPN. After all, it requires a valid email address and some type of digital payment (Bitcoin is accepted). If you want a stronger solution for privacy, and one that accepts cash, consider **Mullvad** (mullvad.net). On their website, you generate an account without providing any personal details. A unique account number is issued to you. Once you make payment for that account number via Bitcoin or mailed cash, the account is enabled. This is likely overkill for most people, but a truly anonymous solution is nice. Current annual pricing for ProtonVPN is $48 and Mullvad is $65. However, your VPN choice should never be based on price alone.

Email Usage Crash Course

All of my clients are given a new primary email address through the service **ProtonMail** (protonmail.com). This free service provides Switzerland-hosted communications with true zero-knowledge data. This means that your email is encrypted from your device before it is stored on their servers. Even with a court order, an employee of ProtonMail would be unable to view your message contents. If an email is sent from one ProtonMail user to another, it is never exposed to interception from a third party. Is this bulletproof? No, nothing is. There will always be some slight chance that an adversary could compromise your communications. However, it is extremely unlikely. On the other side, a court order to Google will hand over all of your account details and email communications stored with them.

While I am not concerned about court orders being executed on my clients' accounts, I am very bothered by data breaches. If a breach occurs at ProtonMail, the thief gets a bunch of encrypted data that is of no use. The breach at Yahoo practically handed over full accounts to the culprit. A big part of being private is simply making better choices, even if they are not fool-proof.

I have a few opinions on email that may not be accepted by the security community. First, email is broken. It is outdated and was never meant to be private. I assume every email I write could be seen by someone else. I also trust services such as ProtonMail over any other mainstream provider. Some will wonder why I don't use Tutanota or other zero-knowledge providers. It is mostly due to adoption. Most people in my circles have ProtonMail and no other secure options. The more messages I can keep within one single encrypted ecosystem the better.

The personal ProtonMail address will be used only for communications associated with your real name. This could include your physician, bank, insurance provider, or any other service that knows your true identity. This is your new primary email account. It will possess a very strong password and two-factor authentication. I prefer Authy for this, as explained previously, but you can find full details with several options at the following address.

https://protonmail.com/support/knowledge-base/two-factor-authentication/

While ProtonMail possess great privacy and security with the default settings, there are things which can be improved. The first is to disable remote images. Many email images contain tracking pixels which identify the IP address and device information when opened. Click on "Settings", "Account", then change "Load Embedded Images" to "Manual". Next, change "Request Link Confirmation" to "Enabled". This will prompt you for authorization to open any links within a message. This prevents accidental link clicking, and displays the entire URL before opening.

Email Forwarding

You likely have a current personal email address that you have been using for several years. This may be a Gmail, Yahoo, Hotmail, or other free provider. I recommend ceasing all outgoing activity from these accounts. However, I never recommend deleting the accounts. If you start using your new ProtonMail account for all of your personal communication, that does not eliminate the need for your old accounts. You will continue to receive desired email through these accounts, and you may need to use an old account to verify your identity to a service such as your bank. Instead of manually checking these accounts, consider forwarding all of your email to your new ProtonMail account.

All major email providers allow you to forward incoming email messages to another address. This allows you to receive the emails being sent to your old accounts without logging in to the services (and providing details about your computer and connection). You will not be able to send email from these old accounts, but that should be avoided anyway. All of your email to old accounts will appear in your new ProtonMail account. Any outgoing message will be from this ProtonMail account. The following steps will forward your email from the old accounts. If yours is not listed, an internet search will provide all you need.

- Gmail: Settings > Forwarding and POP/IMAP > Add a Forwarding Address
- Yahoo: Settings > Accounts > Forward
- Hotmail/Live: Settings > Options > Mail > Forwarding > Start Forwarding

Overall, think of your new ProtonMail address as your primary email account, replacing anything previously used, such as a Gmail account. It should only be used for desired communications. Try to avoid using this address for newsletters and junk accounts. You should consider creating a forwarding account for anything that is not vital to you. You will need additional email services for use with this junk mail. I use a mix of free email accounts from Blur, AnonAddy, 33Mail, SimpleLogin, and my own domains. I will start with Blur.

All of my clients receive a free account from **Blur** (dnt.abine.com). This company provides an email masking service which protects your personal email account. Blur allows you to create numerous unique email addresses, such as jifgfghf@opayq.com, and any email sent to that address will be forwarded to your personal email account. These prevent merchants and services from knowing your real email address, but allows you to receive email communication and confirmation links. I prioritize Blur because of its mobile app which makes email address creation easy and fast.

All of my clients also receive a free account from **AnonAddy** (anonaddy.com). It also provides an email masking service, but allows more leniency with the addresses. AnonAddy defaults to a username-based service. If my username were inteltechniques, any email sent to an address

at @inteltechniques.anonaddy.com would be forwarded to my real email address. For example, any email sent to a forwarding address of junkmail@inteltechniques.anonaddy.com or amazon@inteltechniques.anonaddy.com would be forwarded to my real address on file. Additionally, AnonAddy provides a randomized and completely private address such as 48cd7fa8-o234uyuo245@anonaddy.me. The username-based addresses are created on the fly while the randomized addresses must be generated within their website.

In 2020, I began incorporating **SimpleLogin** (simplelogin.io) into my own privacy strategy. This service offers free and premium tiers, and the free option is usually sufficient for my clients. Similar to AnonAddy, you can choose between a custom keyword username, such as contact.boatkeeper@simplelogin.co, or something random such as 98f11458-7c6f-457f-a045-c58d05ccf70@simplelogin.co. Both allow unlimited incoming messages and outgoing replies to incoming mail, but the free plan limits users to five alias addresses.

33Mail (33mail.com) has been a staple for myself and my clients, but many services now block accounts from this provider. It works much like AnonAddy. You select a username and can start receiving any email messages sent to that account. As an example, if my username were inteltechniques, any email sent to test@inteltechniques.33mail.com would be forwarded to my real email account.

While some clients prefer all messages to be forwarded to their personal ProtonMail account, I prefer to create a second ProtonMail account just for junk that is in an alias name. For ultimate privacy, I believe that all alias email from services such as Blur, AnonAddy, and 33Mail should also be sent to an alias ProtonMail account. Isolation will be a key part of the instructions in future chapters. This will be explained further in the anonymous payments chapter and the anonymous home purchase options. Until then, I will summarize my minimum recommendations for an email strategy at this point.

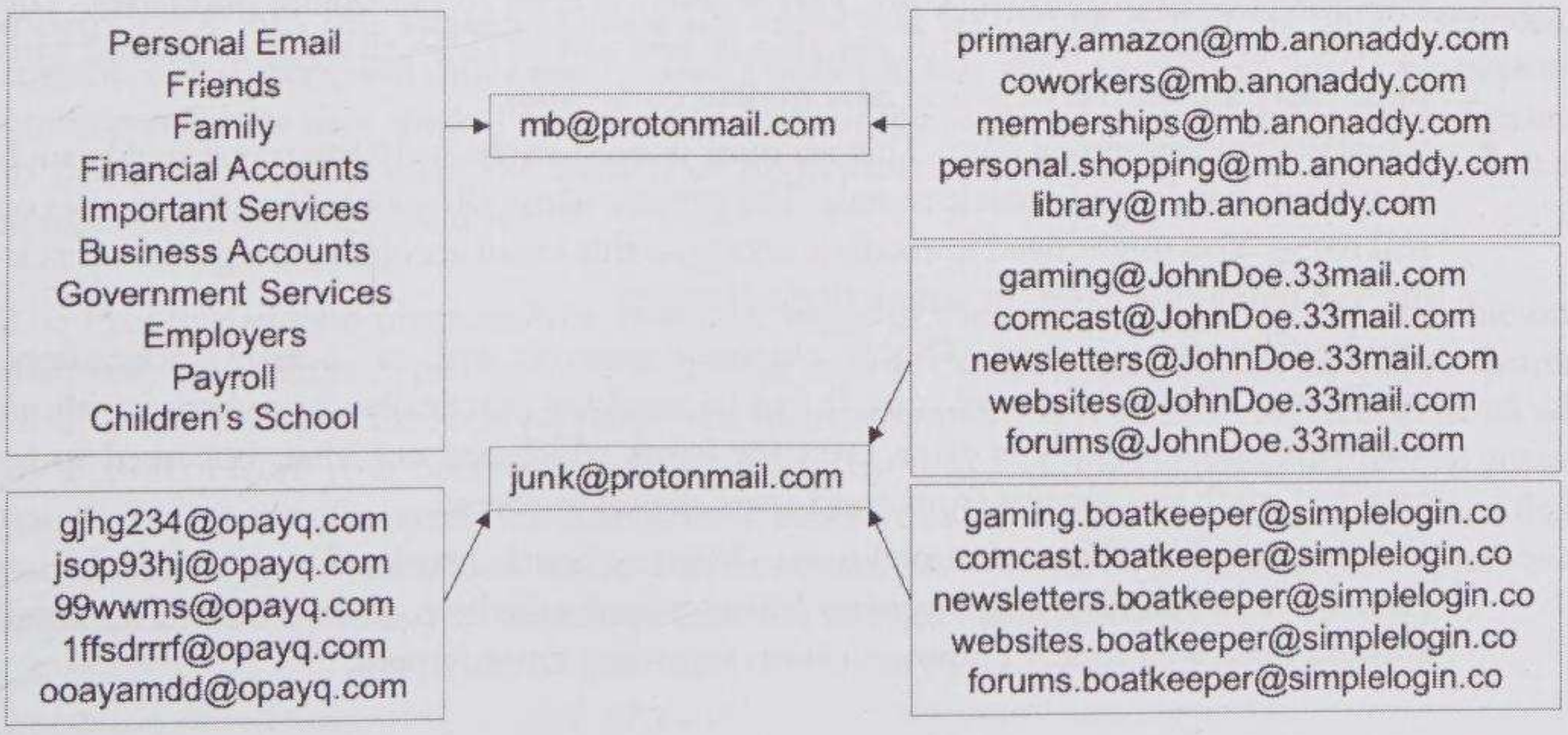
Primary ProtonMail Address: This is in your true name, and may appear similar to the email address of mbazzell@protonmail.com (not my real address). It is used for all personal communications and is the only address associated with important online accounts such as financial, insurance, and employment. Your old personal email accounts forward to this single address. All outgoing mail is from this new address.

Primary Forwarding Address: This is a "junk" account that can be used for items in your real name, but not vital to be received. This could be for accounts with poor privacy policies which share your information with third parties, such as PayPal or Amazon accounts in your true name (we will eliminate these later). It can be a Blur, AnonAddy, SimpleLogin, 33Mail, or other forwarding service. The addresses should not include your real name similar to jifgfghf2jhee11gjhg234@opayq.com, amazon@mynewprivateusername.anonaddy.com, or amazon@mynewprivateusername.33mail.com.

Alias ProtonMail Account & Forwarding Address: This is a second "junk" account which should only be used for items in an alias name. This could be for websites that demand registration in order to view content, newsletters, or anything that does not need your true name. It can be a Blur, AnonAddy, SimpleLogin, 33Mail, or other desired forwarding service which sends incoming messages to a secondary ProtonMail account.

Most importantly, NEVER use a forwarding or masking email service for anything vital. I would never recommend a Blur, AnonAddy, SimpleLogin, or 33Mail address for use with anything related to finances or banking. If these services should disappear tomorrow, you do not want to lose access to anything important. All of these providers have a free and premium tier. Most of my clients only need the free services, but I choose a paid plan for myself. This allows me to take advantage of all services provided and usually offers premium support. Paid AnonAddy plans allow me to send response emails from the alias addresses I create.

Let's pause and take a look at this strategy of email usage. In the following chart, your new personal email address is mb@protonmail.com. It is used for the important things in your life and has replaced the Gmail account you previously had. Any time you need to sign up for something in your real name that will likely send junk mail which is not vital to you, you have the forwarding account of mb.anonaddy.com. When you want to use an alias online, you have the 33mail, SimpleLogin, and Blur addresses at your disposal. These forward to another ProtonMail address exclusively for junk. All of these accounts deliver messages to your single ProtonMail inbox with a paid plan. In my opinion, this represents the minimal coverage you need. In a moment, we will escalate the protection.



Intermediate Email Strategy

I possess a paid ProtonMail account, and I rely on this service for the majority of my personal email communications. The lowest plan costs approximately $50 annually and provides six email addresses. You can choose alias addresses for various needs, and check only one inbox. When I conduct a full reboot for my clients, I generate an email strategy similar to the following, and do not rely on free email forwarding options. I find the simplicity of one inbox and ability to send emails from multiple addresses within a single web client or mobile application to be more favorable to some clients. There is no need to overly complicate things, and convenient options will be used more consistently than difficult tasks.

- Real.Name@protonmail.com: This account is considered a public email address, and is provided to businesses, such as banks, as a primary email address for communication. It is an address that will be publicly visible eventually. Data mining companies and credit bureaus will eventually identify this as your primary email account, which is desired.
- Nick.Name@protonmail.com: This account is exclusively for close friends and family. It is less likely to leak publicly. It can be nice to have isolation between personal life and everything else.
- Alias.Name@protonmail.com: This account is in the name of the alias used by the client. This allows sending and receiving mail in a unique alias name. This can be vital when a home is titled in an alias name and the client wants to have immediate access to email messages intended for that recipient.
- purchases1980@protonmail.com: This account is used for all online purchases. The generic name allows usage with any alias or real name. This will likely be shared with third-party affiliate services and data mining companies.
- travel1980@protonmail.com: This account is used exclusively for travel needs such as airlines, hotels, and vehicle rentals. The generic name allows usage with any alias or real name. You might need immediate access to this email account during hotel check-ins, car rental processes, or airline flight changes.
- number@protonmail.com: This is a generic account with no personal identifiers, similar to 1980@protonmail.com. It can be used for practically any purpose without disclosing any name. It is often used for items which are not vital, but need to be received, such as a receipt from an in-store digital purchase.
- Employment.Name@protonmail.com: Many clients work for themselves or participate in full-time employment. Either way, I ask them all to consider an email address dedicated to any communication regarding employment.

It is important to note that ProtonMail will assign whichever name you provided during registration to each of these accounts. Therefore, log in to your account and navigate to Settings > Account > Select an Address. Select each alias address and modify the actual name as desired. I recommend keeping the generic accounts simple. My travel account is similar to travel1980@protonmail.com and the name associated with it is simply "Travel". When I send an email from that account, the "from" appears as "Travel (travel1980@protonmail.com)".

The next step I recommend is to create folders for every alias. This will make it easier to identify which email is associated with a specific account. Navigate to Settings > Folders/Labels > Add Folder. Create a new folder for each email account. Next navigate to Settings > Filters > Add Filter. Create a new filter for each email address. The following is an example which will route all mail to travel1@protonmail.com to the folder I created titled Travel1.

Name: Travel1
Conditions: If the recipient is exactly travel1@protonmail.com
Actions: Move to Travel1

Repeat this for each email alias. When finished, you should have all alias accounts listed in the lower left corner of your email page. You can now easily identify which alias account received a message, and will be less likely to respond as your real name. No messages will appear in your global inbox, which provides isolation.

Email forwarding services such as Blur, AnonAddy, SimpleLogin, and 33Mail could also be incorporated into this strategy. Unless my client will be joining numerous online services, forums, newsletters, and other annoyances, I prefer to stay away from these unless the person understands how they work. I find the simplicity of the single inbox with numerous addresses to be more beneficial than the burden of numerous forwarders. The only downside is the annual expense for the paid tier.

The ProtonMail paid plans include unlimited usage of the Import-Export utility available on their website at https://protonmail.com/blog/import-export-beta/. This tools easily exports all of your messages for archival purposes. More importantly, it allows you to import all of your content from your previous email provider. If you had a Gmail account for several years, you likely possess messages which need to be accessed on occasion. You can import all of this content into your ProtonMail account for easy access without logging in to your previous account(s). Be sure to pay close attention to the storage requirements.

Advanced Email Strategy

If the previous two scenarios do not quite scratch your itch for ultimate digital privacy and security, I present the strategy I use for my email communications. It is a bit extreme, but provides a new level of digital security which is missing from the previous examples. In both of those, you are relying on third-party services outside of your control for your email communications. This alone is not that bad, as we always rely on SOMEONE to host our email. What if you should lose your access to that account? In those scenarios, I chose ProtonMail as my email provider. What if they disappeared, terminated your account, or suspended your access due to suspicion of fraud? While all of this is extremely unlikely, the chance still exists. Therefore, I prefer to take advantage of the secure hosting provided by ProtonMail while controlling the avenues of communication with my own domain. This will require several complicated steps, but the end result is worth the effort.

First, a paid ProtonMail plan is required in order to bring in your own domain. I prefer to pay via Bitcoin, but an "anonymous" debit card could also be used (both are explained in Chapter Nine). A paid domain registrar is also required in order to secure a custom domain name. For domain registration, I prefer Namecheap. However, I do not recommend any of their other products. I find their web hosting to be awful compared to other providers, but their domain services are ideal. Namecheap provides affordable domains and includes their own WhoIsGuard service for free. This masks your registration information from public view. Some registrars charge up to $20 annually for hiding these details. Our first step is to secure a domain name. What should you choose? Here are three considerations.

- **Don't Choose Your Name**: You may be tempted to secure your real name within the domain, similar to michaelbazzell.com, but this has many disadvantages. While it works well when giving out an email address while using your true identity, it appears suspicious when trying to use an alias. Bob.Smith@michaelbazzell.com would raise some eyebrows and give away your real name.
- **Keep It Generic**: I prefer a domain name which could be associated with any real or alias name I choose. I also prefer to stay away from privacy-themed domain names, as they can also raise suspicion during online purchases. Generic domains including the term "mail" work well for me. During this writing, I purchased the domain "securemail.work" from Namecheap for $2.88 with a $6.88 annual renewal. Trying to obtain a short domain name with a ".com" extension can be difficult as most good options are taken. I can now be myself with michaelbazzell@securemail.work, create an alias email account such as bob.smith@securemail.work, or become generic such as office@securemail.work.
- **Top Level Domain (TLD)**: There are many ways to end your domain such as .com, .net, .biz, etc. In the previous example, I chose ".work" in order to test my strategy cheaply. However, this extension may confuse people. If you are choosing a domain

name which you will use for many years, a ".com" TLD is probably most appropriate. For daily use, I rely on inteltechniques.com for all work email.

During checkout, Namecheap will demand to know your real name and physical address. While they do not share this publicly, they can sell and share it with third-party partners. Using John Doe at 1212 Main Street will earn you a quick account suspension from Namecheap, as false information violates the rules imposed by the Internet Corporation for Assigned Names and Numbers (ICANN). Their policies require you to be honest about the details you provide. This puts us in quite a predicament, but I have a solution that may work well for some.

During my purchase, I created a new Namecheap account, provided my first name as "M", my last as "B", and placed my order with a Privacy.com card (Chapter Nine). During checkout, Namecheap demanded a full name, physical address, telephone number, and email address of the registrant for the domain. While you could lie on each of these, you risk losing the domain and you would be violating ICANN rules. Instead, I again provided "MB" as my name, and the full mailing address of the hotel where I was staying at the time. I even included the room number in order to be transparent. Technically, this was my current physical residence. I supplied an AnonAddy forwarding email address and a VOIP telephone number which I could access if needed. I executed the purchase, and my new domain was generated. My total cost was $3.06. I provided my true initials, my true current physical address, an email address which forwarded to my ProtonMail inbox, and a VOIP number which forwarded messages to my email. I believe all of these details were accurate at that moment in time, and I violated no ICANN rules. You may disagree.

Next, I needed to configure this new domain to forward messages to my ProtonMail account, and configure my ProtonMail account to receive the messages sent to that domain. The following steps walk through the process at the time of writing.

- In the Namecheap dashboard, I clicked the "manage" button next to my new domain.
- In ProtonMail, I clicked "Settings", "Domains", then "Add Custom Domain".
- In the ProtonMail pop-up menu, I entered securemail.work as my domain.
- In the Namecheap Domain settings, I clicked "advanced DNS".
- I then clicked "Add New Record" in the "Host Records" menu.
- As instructed by ProtonMail, I chose "TXT Record", "@", and the values presented in the ProtonMail configuration pop-up within the Namecheap settings.
- In the ProtonMail dialogue, I clicked "Next".
- In the "Add Addresses" dialogue, I entered EP@securemail.work and a name of Secure Mail. I clicked next and allowed ProtonMail to generate my new keys.
- I clicked the "MX" button in the ProtonMail configuration menu.

- In Namecheap, I chose "Custom MX" in the Mail Setting menu. I then provided the custom settings displayed in the ProtonMail dialogue, visible in Figure 3.04.
- I added the SPF record into Namecheap as instructed by the ProtonMail dialogue.
- I added the DKIM record into Namecheap as instructed by the ProtonMail dialogue.
- I ignored the DMARC options and closed the ProtonMail pop-up window.
- When finished, I checked the "Catch All" option next to my new email address.

Within two hours, all of the settings were applied and ProtonMail was happy with my configuration. Figure 3.05 displays my TXT records, which were applied with the previous instructions.

Type	Host	Value		TTL
MX Record	@	mail.protonmail.ch.	10	Automatic
MX Record	@	mailsec.protonmail.ch.	20	Automatic

Figure 3.04: MX records for a custom domain.

Type	Host	Value	TTL
TXT Record	@	protonmail-verification=[redacted]	Automatic
TXT Record	@	v=spf1 include:_spf.protonmail.ch mx ~all	Automatic
TXT Record	protonmail._domai...	v=DKIM1; k=rsa; p=[redacted]	Automatic

Figure 3.05: TXT records for a custom domain.

Let's pause and reflect on what we have accomplished. I purchased a domain name of securemail.work semi-anonymously. The details of this registration are hidden from the public. I created a paid ProtonMail account. I forwarded the mail servers of the domain name to the ProtonMail service. I configured both a real email address and a wildcard address within ProtonMail. Any email sent to my domain is received in my ProtonMail account. If you send an email to EP@securemail.work, 12@securemail.work, or ihatethisbook@securemail.work, it will get to me. I can provide an unlimited number of email addresses for this domain, and all will end up in my inbox. This is very similar to the way email forwarders work, but I have all control.

I can also incorporate the techniques mentioned in the previous strategies. Any email forwarders I use can be sent to either a real ProtonMail address or a securemail.work address. I can import my old email from another provider and export all content to possess a full backup (explained in a moment). My email content is stored as encrypted data, and no one at ProtonMail can view my messages. I have a mobile app on my phone which accesses my ProtonMail account, and the web interface is available through my browser. I can send and receive mail from accounts in this new domain name. If ProtonMail should ever become unavailable, I can forward my domain within Namecheap to a new email provider and continue to access my accounts.

Practically every email I send is from an address of my own domain which I own. If sent to other ProtonMail users, the content never leaves their systems and stays fully encrypted to the recipient. I believe it is vital for extreme users to own the domains which are used for emails. It looks more professional and gives you permanent control of the content. You can have the best of both worlds with a custom domain within ProtonMail.

Encrypted Calendar and Contacts

In 2020, ProtonMail began offering an encrypted calendar service. I believe that possessing an encrypted, zero-knowledge calendar is more vital than private email. Consider the amount of sensitive information stored in your calendar. Your doctor appointments, blind dates, work schedule, job interviews, and travel plans disclose a lot about you. The details entered within the notes of these entries can identify your location, medical history, or desire to leave your current employer. Do you want all of that data visible to Google or Microsoft? I know I don't. Therefore, my calendar is protected through ProtonMail and only visible to me.

ProtonMail has always supplied encrypted contacts as part of their email packages. These details are also extremely sensitive. I would never want to expose the cellular telephone numbers, home addresses, and employers of my friends and family. Storing this content within products provided by companies which make profits from data sharing is irresponsible. The default configurations of ProtonMail's calendar and contacts is sufficient for most, but I prefer to make one modification.

- Settings > Account > Automatically Save Contacts > Disabled: By default, ProtonMail saves the contact details of any outgoing messages, including responses. This leads to a contact list full of people who are rarely contacted and leaves potential evidence of sensitive associations. I prefer to disable this option completely.

ProtonMail Alternative (Tutanota)

I mentioned Tutanota briefly in an earlier section of this chapter. They provide a very similar service to ProtonMail and I believe that you could replace "ProtonMail" with "Tutanota" in most of the previous details to produce a similar result. Tutanota also delivers end-to-end encrypted email, contacts, and calendar services. They are based in Germany and have a strong history of respect for privacy. However, they are based in a Fourteen Eyes country, which may make a few readers nervous. They provide a mobile application and have a nice web-based interface.

Why do I choose ProtonMail over them? Adoption. Currently, 70% of email correspondence from my ProtonMail account is to other ProtonMail users. Less than 5% is to Tutanota addresses. Therefore, it simply makes more sense to stick within the ProtonMail ecosystem (for now). Tutanota offers a free tier, and I encourage you to create an account and test their services. I have found their web interface to work well, but the mobile app is quite slow.

Account Summary

Hopefully you now have an email, calendar, and contacts solution which is private and secure. We should bring absolutely nothing from our past life into our new private life. Once you have new hardware and new accounts for communication, my preference is that you never access the old accounts from your new devices. The previous forwarding strategies are fine, and should work without logging in to your old accounts. This is especially important for mobile devices, and I insist that Google apps are never installed anywhere. This would immediately associate the new device with the old Gmail account, and ruin the isolation created.

I realize that the previous email strategies can seem overwhelming. This is why I present them as basic, intermediate, and advanced options. Privacy is a marathon, not a sprint. Each step you take makes you more private and secure. You can always upgrade your strategy once you have an understanding of the basics. You may also tweak pieces of each option and create your own solution. My goal is to simply present numerous ideas to aid in your own execution.

I encourage you to begin visually creating your own email strategy. I often draw diagrams, using pencil and paper, until I have created a workflow that makes most sense for a specific client. This may seem archaic, but the visual representation helps me. My overall strategy has changed considerably since I began this journey. I would anticipate changes to your own plans as your digital life is hardened.

Data Archiving

Whether you use a Mac, Windows, or Linux machine, I highly recommend possessing a backup of all email, calendars, and contacts. I mentioned Mac options in the previous section, but I only rely on those strategies when a client insists on using the stock Mac apps. Personally, I do not store my email, contacts, or calendars within any Apple application. This is because Apple constantly sends data home to their servers, regardless of your iCloud or Apple ID settings. I do not want to take the chance of unknowingly sending sensitive details to Apple as part of their analytics collections. Therefore, I rely on an open-source third-party solution called **Thunderbird** (thunderbird.net). This product, which is made by Mozilla, is a very minimal and somewhat ugly email, contacts, and calendar application. I do not recommend using it for daily access to these services, but only as an archiving solution to make sure you always have a copy of your data. First, let's discuss why this is so important.

Consider your primary email account. What do you possess inside of it? You likely have years' worth of valuable emails, important documents, priceless photos, and evidence of practically every online account. Could you replicate your contacts list from memory? Do you know all of your upcoming appointments without relying on your online calendar? What if it all disappeared tomorrow? If your service unexpectantly shut down, kicked you out, or was "hacked", you would not have access to all of this data. This is why everyone should always possess a full backup of all of this content.

If you use Fastmail, Gmail, or any other standard email service, you can connect through a protocol known as IMAP. Clients such as Thunderbird allow you to specify the settings of your accounts, and then keep your entire email, contacts, and calendars synced to your computer for offline use. If your online accounts disappear, you still have access to your offline copies of all the data. Every reputable email service provides tutorials for connecting your client, such as Thunderbird, to their service via IMAP. Calendars sync via CalDAV and contacts sync via CardDAV.

Encrypted email providers, such as ProtonMail, present a difficult scenario. Since the email is fully encrypted, they do not allow standard IMAP access from a third-party client. However, ProtonMail addresses this with their bridge and export applications. Available only to paid accounts, these utilities allow an email client to download all messages from their servers. This provides a full backup, the possibility of offline access, and full search capabilities within the content of the messages. You can find full details for download, installation, and configuration of the Bridge client at https://protonmail.com/bridge. It supports Thunderbird natively. The export client is still in beta, but available to the public on their blog. Regardless of your chosen email, contacts, and calendar strategy, please make sure you have a continuously updated backup of your data. Hopefully, you will never need it. Once configured, sync your content weekly and verify you can access the data without an internet connection.

File Sharing

Occasionally, you may need to send large files to someone remotely. Most email providers have a 25MB limit on attachments. If you need to transmit a 750MB video, large PowerPoint document, or any other file exceeding the email limits, consider the free option **Firefox Send** (https://send.firefox.com). This service allows you to upload a file up to 1GB in size and generates a link to share. The recipient to whom you provide the link has only 24 hours to download the file. It is permanently deleted after the first successful download or the 24-hour limit, whichever happens first. Furthermore, the content you upload is protected with end-to-end encryption. This prevents Firefox employees or anyone else with server access from the ability to see your content. This system is not perfect, and I would never use it for extremely sensitive content, but it works well for daily sharing tasks.

Notes

Applications such as Evernote, OneNote, and Apple's iCloud Notes are extremely convenient. They also store your sensitive content in an unencrypted state for employees, criminal hackers, and third-party companies to abuse. I never recommend any of these services to clients. Instead, I rely solely on **Standard Notes** (standardnotes.org) for all of my notes and task lists. This service, with free and paid tiers, provides an elegant application for all major platforms, including mobile devices. All notes are end-to-end encrypted with zero-knowledge from the provider. The free plans are sufficient for most users, but power users may want the paid features. Notes updated on one device synchronize securely to all other devices. Many of my clients share a single account with multiple family members as a way to keep track of upcoming events and tasks. I have never reached any limits of sharing a single free account with multiple devices. My notes, outlines, and "to-dos" for this book were stored completely within Standard Notes at all times.

Traveling with Devices

When you travel, especially internationally, you increase your chances of an encounter with a government official who demands access to your data. This could be an extremely minimal risk during a traffic stop while being suspected of drug trafficking, or a much more likely scenario of being intercepted while entering another country. Regardless of your likelihood of being detained and questioned, you should be prepared for an unfortunate encounter. When I travel, I assume that I will be asked for access to my data at some point. Therefore, I prepare for this possibility in advance in order to avoid temptation to submit to a search of my data.

Some may fall back on the "I have nothing to hide" argument when being asked by an immigration official for full access to personal devices. I believe it is very inappropriate to hand over your data to any third party, especially a foreign government upon entry into a new

territory. Many countries are embracing new technology such as Cellebrite forensic acquisition devices which suck up all data from a mobile device in minutes. This data is stored indefinitely, and likely insecurely. The country you entered may have little interest in the data they collected about you, but the intruder who later steals that data can abuse it without your knowledge. My preference is to avoid any data collection which may violate my privacy.

Domestic Travel (Vehicle): I have never encountered a situation while driving throughout America where my data was in jeopardy. I obey ~~all~~ most traffic laws and try to minimize any interest from law enforcement. I keep all of my data encrypted and backed-up, so theft is not a huge concern. Unless you are under arrest, or a search warrant has been issued, law enforcement has no right to take custody of any devices. If you are under arrest, a search warrant will be required to legally extract the data from any confiscated devices. Consent may be requested, which you can deny. If probable cause that you have committed a crime has been established, you begin to lose your rights to privacy. If a search warrant for your devices has been obtained, you have big problems.

Currently, the Cellebrite I mentioned previously is suspected to have the ability to bypass the encryption of both Android and Apple devices. This is usually short-lived, as device manufacturers and forensic companies play cat-and-mouse with their abilities to protect data and defeat encryption. Some judges have ruled that fingerprints CAN be obtained by police in order to unlock a phone (U.S. Supreme Court Riley vs. California) while other magistrates declare that officials CANNOT force you to give up biometrics (U.S. Northern District of California Case # 4-19-70053). In other words, there is no clear answer. This is one reason I require a PIN to unlock my iPhone. I have the fingerprint and face identification options disabled.

Readers who are in law enforcement may scoff at my remarks here, but there is no ill-intent. As a retired law enforcement officer, I understand that people can get caught up in investigations surrounding illegal activity without committing any crimes. In 2016, I was in a vehicle driven by a ride-sharing contractor, hailed through the official mobile application for that company. After picking me up, the vehicle was stopped by under-cover police detectives and the driver was arrested. He was wanted on serious drug conspiracy charges and likely headed to prison. Understandably, the detectives questioned me sternly at the scene of the arrest. I was able to explain my presence, display visual proof of the hired ride on my device, and justify that I was not involved in their investigation. However, a detective requested to connect my device to a Cellebrite in order to prove my innocence and later critique my story if needed. I declined consent to the data acquisition, which was met with great skepticism. I politely explained my former career and stance on privacy, and insisted I would not voluntarily grant access to my device. My retired badge and credentials likely aided this conversation, which may seem unfair to civilians in the same predicament.

I completely understand the request for my data, and I would have probably acted similarly when I was investigating felony and federal crimes. On the surface, I appeared to be connected to a major felony drug trafficking investigation. Detectives must exhaust all investigation tactics, which includes a thorough look into anyone contacted during the arrest. I was in the wrong place at the wrong time. If I had allowed my device to be extracted, the data would have been stored at the police department; provided to the prosecutor and defense during the discovery process; and accessible to countless attorneys, clerks, interns, and the defendant. I lose all control, and my identity, messages, emails, contacts, and history could be exposed publicly. Realistically, no one would have paid much attention to me as I was cleared in the investigation. However, I simply refuse to expose my personal data.

This may all seem far-fetched, but scenarios such as this play out every day. This is why I enable the best possible encryption I can on any devices with me while I travel. This includes laptops. I will obey all legal demands, I will cooperate with law enforcement, but I will not unnecessarily associate my personal data with unrelated investigations. If you find yourself in a similar situation, I encourage you to be polite and helpful, but also to understand your rights and know your boundaries for consent. You can't call them later and ask them to delete the data.

Domestic Travel (Air): I fly a lot throughout America, and I pass through Transportation Security Administration (TSA) checkpoints more than I desire. I remove my laptop and mobile device from my bag, place them in the worn grey containers, and hope I am not pulled aside for secondary inspection. Fortunately, I have never been asked to unlock my devices during domestic air travel, but I know others who have. Prior to 2010, TSA agents were asking people to unlock their laptops and mobile devices as proof they functioned properly. This was due to a specific threat about explosives being stored within electronic devices. I have never heard of any data acquisition during this time, which was short-lived. The greater concern is the reported incidents where domestic travelers were required by TSA to unlock their phones and these devices were taken out of sight of the civilian for several minutes. There is speculation that TSA possesses mobile device forensic acquisition units, but I have no evidence of this.

TSA officials have responded to these allegations stating it "does not search electronic devices for electronic content that may be contained on the device, and does not extract data from passenger electronic devices" and that physically analyzing the devices "is solely intended to verify that there has been no physical tampering or hidden threat placed within the electronic device".

In my experience, your chances of being asked to unlock any type of device during domestic travel is extremely rare. I almost always travel with my primary laptop (full-disk encryption) and my travel mobile device (iPhone with default encryption and 12+ digit PIN). The role of

the TSA is to scan people and luggage for physical threats. Any interest in your data will likely be very targeted and searches would probably be conducted by another organization such as U.S. Customs and Border Protection (CBP). That brings us to international travel.

International Travel (Vehicle): This is where things can get tricky. The moment you leave one country and enter another, you are at a higher risk of data interception and acquisition. When leaving America and entering Mexico via vehicle, your chances of any demands to access your devices is very minimal. This can change if you are on a "list" of suspicious individuals, but most people should have no issues. Canada is a different matter. I have found the Canada Border Services Agency (CBSA) to be more scrutinous than most other countries.

In my experience, entering Canada by vehicle provides just as high of a likelihood of secondary screening as air travel. Many people refer to their "rights" prohibiting the search of their devices, but this is inappropriate thinking. You can absolutely refuse to allow a search of your data at the Canadian border. In return, Canada can refuse you entry into the country. If you are demanded to unlock a device and refuse, you will not likely be arrested. You will simply be shown the way back across the border into America.

For the record, I have never received a demand to unlock a device by the CBSA. I have received my share of secondary interrogation due to some questionable border crossings, but my devices were never compromised. However, the CBSA is fairly transparent about their rights to inspect the content on your devices. The CBSA can search any device entering the country without any specific suspicion. However, CBSA policy states that officers should only "take a quick look" at each document before moving on to the next. For example, they should only look at documents or photos "for long enough to determine that they do not contain contraband such as child pornography or hate literature". If the CBSA officer sees something that raises their suspicions, a more thorough search may be conducted. CBSA agents can also demand a password or fingerprint to unlock a phone. The Canadian Customs Act states that travelers are required to "open or unpack any package or container that the officer wishes to examine". The CBSA points out that not handing over a password could create a variety of problems, including denial of entry into Canada.

Fortunately, CBSA agents cannot always download photos, text messages or emails from the device. According to the British Columbia Civil Liberties Association (BCCLA), "If the CBSA wants to search information on the phone that is only accessible once it is connected to the cloud, the agency must first obtain a warrant issued by a judge". However, this provides little protection. The CBSA's policy is that officers should set the device to airplane mode before searching to "reduce the possibility of triggering remote wiping software, inadvertently accessing the Internet or other data stored externally or changing number versions or dates", according to internal guides.

Officers are allowed to read emails which have been downloaded and opened, and they are supposed to assess this by seeing whether the emails have been marked as read. The BCCLA assumes this also applies to text messages. Agents can also copy the contents of the device or keep the phone for further inspection. The Customs Act gives the CBSA the "power to detain goods if the officer is not satisfied that the goods have been properly screened for admission into Canada, including the contents of electronic devices", according to the BCCLA guide. Because of these issues, I follow a strict personal set of rules when traveling to Canada, which will be explained after the next section.

International Travel (Air): You are at most risk of a demand to unlock and present your data when you are traveling via air to other countries. You basically have no rights. Some locations in the middle east or near China may be more demanding toward seeing your digital content than popular European countries which are targeted by tourists. Regardless of your destination, you are always at risk of being denied entry if you refuse to allow a border agent to inspect your unlocked devices. Therefore, I possess a very specific protocol for ALL travel outside of the United States.

Laptop: I almost always bring a laptop when I travel internationally. Whether for my own work or to be used during a presentation, I simply need a computer with me at all times. When leaving my country, I make an assumption that I will be forced to unlock the device at any border. First, I completely wipe out my Debian Linux machine and install a fresh copy. I enable full-disk encryption and install any software necessary for my trip. I do NOT load any personal data. While still at home, I identify all of the personal data I may need such as my password manager, client documents, PowerPoints, etc. I encrypt these into a VeraCrypt container and store the container in my SpiderOak account, which is zero-knowledge with end-to-end encryption. If I am asked to unlock my laptop, I do. There is no personal data on it, and nothing sensitive to be exposed. When I arrive at my final destination, I download the VeraCrypt container and place it on my device. Before I leave the country, I wipe the hard drive and re-install Debian Linux from a USB drive containing the official ISO file.

Mobile Devices: When traveling in North America, I usually bring my travel iPhone. However, I do not bring the SIM card. The device basically has no internet connectivity. I then force close all of my apps and make sure I am logged out of everything. If I am forced to unlock the device, my email and communication apps will only load a login screen. Once in Canada or Mexico, I purchase a new SIM and log in as necessary. I repeat the process when leaving. When traveling outside of North America, I never bring a mobile device. I can use my laptop for almost all of my communication needs. If I need a mobile device, I can purchase an affordable "burner" with a new SIM card.

Some may believe that possessing a hidden partition on a laptop or a hidden VeraCrypt container would eliminate the need to upload and download the data. I disagree with this tactic

as some border agents are trained to look for this data. If you are found to possess anything "secret", you are more likely to be denied entry or detained. I prefer to enter "clean" and simply not worry about anything. Some will argue that you appear more suspicious if you enter a country without a mobile device. I have never received any resistance with this. My valid response is that I have no service in the country I am entering, so I did not bring my phone. Obviously, your mileage may vary.

The final consideration is the border crossing into the United States. If you are a U.S. citizen, you will likely be waived through with little hassle. If you are not a citizen, expect issues. The U.S. has some of the most invasive privacy practices when it comes to entry by foreigners. You may be asked about your social networks and email accounts, and be prone to the search of your devices. The lessons explained previously may be beneficial.

Tor Browser (https://www.torproject.org)

You may be wondering why I did not mention the Tor Browser during the previous private web browsing section. This software has many valuable privacy-related uses, but also just as many hindrances. First, we should understand what the Tor Browser does. It is open-source software for enabling anonymous communication over the internet. It directs all internet traffic through a free volunteer network consisting of thousands of international "relays" to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis. Similar to a VPN, the Tor network disguises your identity by moving your traffic across different servers, and encrypting that traffic so it is not traced back to you. The Tor Browser is free and can be downloaded on Windows, Mac, and Linux. It relies on a hardened version of Firefox and appears similar to a standard browser in many ways.

The Tor Browser is present on every machine I use, but I do not use it every day. In fact, my hardened Firefox browser receives far more usage than the Tor Browser. This is due to many hurdles associated with web browsing over the Tor network. Any time you connect to a website while using the Tor Browser, that site absolutely knows you are on the "anonymous" Tor network. Unfortunately, there is a negative connotation associated with Tor. Many companies still believe it is mostly used by online drug dealers, credit card thieves, and criminal enterprises. While crime is still very present within the Tor network, it is no longer the majority of traffic. Many traditional sites will scrutinize traffic from this network and present difficulties while attempting normal internet usage across standard websites. Many websites present multiple captchas from Google in order to load a page. Online marketplaces such as Amazon tend to block payments. Some web firewalls throttle traffic from Tor users making it difficult to load web pages. Many social networks suspend accounts after a Tor-enabled connection. Because of these reasons, I am hesitant to encourage clients to make the Tor Browser their primary internet connection. However, I stress the importance of possessing this option and relying on the Tor network in the following scenarios.

- International Travel: There are many countries which block access to VPN connections. Furthermore, many public Wi-Fi connections block VPN software from securing a private connection. In many of these instances, the Tor Browser will bypass these restrictions. You may need to reconnect many times until you find a connection which is allowed and not blacklisted within an internal database.
- Sensitive Content: My job requires me to investigate dark areas of the internet. If I expect to encounter criminal activity, stolen data, or counter-surveillance, I am always connected through the Tor Browser (on my VPN-protected machine).
- Tor Content: There are thousands of websites which can only be accessed within the Tor network. This browser can access these sites as well as all open internet sites.
- Restricted Content: Some public networks filter internet traffic such as dating websites, social networks, and mature content. My library blocks Craigslist for some reason. Some countries block news or content which contradicts their own agendas. In 2019, Russia was blocking access to ProtonMail. Tor eliminates these roadblocks.

If you anticipate extensive travel to countries which block open internet access, I would configure a pluggable transport within the Tor Browser before travel. I use **Meek**. Meek is an obfuscation layer for Tor designed to evade internet censorship. Traffic is relayed through a third-party server which is difficult to detect and block. More details can be found on the official Tor website at https://trac.torproject.org/projects/tor/wiki/doc/meek.

Summary

- New clients receive all new devices and any forced registration is in an alias name.
- Full encryption is mandatory on all devices including portable storage.
- Stock browsers should be replaced with custom options.
- Password managers are vital, and I prefer offline storage.
- Old email addresses should be forwarded to a secure new account.
- Clients need multiple email addresses within a single login.
- Consider potential data invasions while traveling.

You can never have privacy unless you possess secure digital devices and connections. This chapter is the backbone for all of the upcoming work you will complete in order to become invisible. As a final note, please remember that technology changes quickly and often. The exact digital tutorials explained in this book ~~may~~ will become inaccurate over time. If you encounter differences during your replication of the steps, online research of the topic should quickly identify new solutions. Later in the book, I present the next level of digital strategies.

Chapter Four

Nomad Residency

I originally hesitated placing this chapter so early in the book. It is extreme to say the least. However, the strategies defined in this chapter can play a strong role throughout the remainder of this book. If the information you are about to read seems too complicated or inappropriate to your life, I completely understand. It is not for everyone. However, I ask that you stick with it, as many techniques discussed later do not require you to become a "nomad".

Traditionally, a nomad is a person without fixed habitation. It is a person who is always on the move and wandering from place to place. Throughout history, food sources and weather were reasons to be nomadic. Today, it may just be the most private option you have. If you are homeless, have no assets, and can fit all of your belongings on your back, the nomadic life can be very easy to implement. I doubt that is your scenario. Fortunately, you can become an official nomad and continue your normal life with assets, credit, government identification, and a traditional lifestyle.

Think about retirees that adopt the recreational vehicle (RV) lifestyle. They head south in the winter and back north in the summers. They are always on the move and do not often possess a traditional physical residence. What state do they live in? Who issues their driver's licenses? How do they get their mail? The nomad life is easier than ever, and you can establish a great level of privacy by executing your personal nomad strategy.

A nomadic life may sound like a drastic change, but selling your home to buy an RV is not required. Before I proceed, I should take a moment to acknowledge situations where this strategy is not appropriate. If you are a government employee living in California, but plan to become a legal nomad in Texas, it just will not work. If you own a home in your name in Illinois, are employed full-time in Illinois, and have children in a public school in Illinois, you will face problems. In each scenario, your Texas driver's license or state identification will not suffice. If you are in a similar situation, don't worry. There are many more privacy strategies in the coming chapters. I want to start here because it is by far the most powerful option.

A previous chapter explained the use of a PMB as a "ghost address". These are basically mail drops that will forward any items to you at any other address you provide. These allow you to give out an address that is not actually associated with your home. I specifically recommended the service Escapees with a presence in Texas and South Dakota. Previously, I only focused on the mail receiving aspect of a PMB. This option can also be used to obtain a driver's license,

register to vote, or renew a passport. You can use these addresses for official government documents or official government identification. There are many steps we need to take, and it won't always be easy. However, the final outcome will provide a lifetime of privacy.

Think about the number of times you are asked for identification. Every time you check into a hotel or rent a vehicle, the name and address on your identification must match what was provided during the registration. The moment this address is entered into any computer system, you take a chance of it leaking into other databases. Often, this leak is intentional and the company that provided the data is financially paid for the information. Your name and home address then appear in data mining company databases and eventually on people search websites on the internet. Becoming a nomad eliminates much of this risk.

In almost every state, you are not allowed to display a PO Box as your address on your driver's license. States which do allow this demand to know your true physical address and share that information with other entities. If you become a legal nomad in Texas or South Dakota, your PMB address is what appears on your driver's license and practically every other document associated with your name. This PMB address is a physical location which you will never visit, but it will be your official residence. This may be the first task that you scoff at, but I assure you it is completely legal. Thousands of people have already caught on to the nomad bandwagon. I have spent five years trying to identify the best methods of accomplishing this, and I believe I have perfected the execution.

First, you must be in a situation where a specific state other than Texas and South Dakota does not have rights to you as a resident. In the spirit of extreme privacy, I will assume that you are ready to relocate, leave your current residence behind, and embrace the idea of extensive travel. The most common type of client in this situation is escaping an abuser and unsure where he or she will make a permanent home. This person knows that leaving behind the current state of residence is mandatory. Nomad residency can be a temporary or permanent solution. I have had clients who use this as a transition toward permanent residency in a desired state. I also have many clients that are still nomads today.

Next, you must choose the state of your future residency. As you will read, there are many considerations before committing to a specific state and its rules. Every situation is unique, and your best option may not be my desired solution. Please read this entire chapter twice before making up your own mind. While you can reverse any actions you take, it will be inconvenient, expensive, and unnecessary. Let's compare some key details of each option in the following two pages.

South Dakota

Vehicle Tax: South Dakota has a 4% vehicle excise tax, but no other sales tax to pay when purchasing a vehicle.

Vehicle Registration: South Dakota vehicle registration fees are based on the year of your vehicle. The renewal month is based on the first initial of your last name.

Vehicle Inspection: South Dakota does not require vehicles to be inspected for safety or emissions.

Vehicle Insurance: Liability and full coverage vehicle insurance is fairly low, but not the lowest in the country. South Dakota is traditionally lower than Texas.

License Fees: A new driver's license costs $28 and only needs to be renewed every five years. The renewal fee is $20. You must physically respond to the DMV to renew after your first online renewal. A South Dakota driver's license can be renewed once by mail without physically being present in the state.

Jury duty: If you register to vote, you have the potential of being called for jury duty. South Dakota is very understanding of full-time travelers and usually offers an exemption from jury duty.

Concealed Carry Permits: South Dakota's resident permit is honored by 30 other states and is valid for four years. You must be a minimum of 18 years of age and the cost is $10. A temporary permit is issued within five days of the date of application. Within seven days of the issuance of the temporary permit the sheriff will submit the application to the Secretary of State who issues the official permit. If you are a PMB holder rather than a permanent resident in South Dakota, you must spend at least 30 days in the state before applying for a concealed carry permit. Under the South Dakota Sunshine Law concealed carry permit information is not considered public information. Many people for whom concealed carry is an important factor have decided against using South Dakota. Because South Dakota issues permits to persons 18 years of age and older, their permit is not recognized by many states. Furthermore, many full-time nomads have no desire to spend thirty consecutive days in the state in order to meet the letter of the residency requirement before submitting their concealed carry application. I present more details about this in Chapter Fifteen.

State Income Tax: None

Texas

Vehicle Tax: Texas has a 6¼% vehicle sales tax. They also charge $90 if you bring in a vehicle that was previously registered in another state.

Vehicle Registration: Texas vehicle registration fees are $50.75 yearly, regardless of year manufactured.

Vehicle Inspection: Texas requires every vehicle to have a yearly safety inspection at a cost of $14.50 annually. If the vehicle is new, a two-year inspection can be obtained for $23.75. Some counties also require a free yearly emissions test. This will require having the vehicle in the state at least once per year. Out-of-state vehicles can often be tested wherever they happen to be located, and the results can be submitted with the application.

Vehicle Insurance: Texas liability and full coverage vehicle insurance is about average for the country. Of the two states that I considered, it is the higher.

License Fees: A new driver's license costs $25 and only needs to be renewed every six years. The renewal fee is also $25. A Texas driver's license can be renewed once by mail without physically being present in the state.

Jury duty: If you are called for jury duty in the county of your official residence, you will not be exempted solely because of your traveler status. A letter to the court identifying your current location (city and state) may excuse you, but there are no guarantees.

Concealed Carry Permits: Texas' resident permit is honored by 38 other states and is valid for four years (the initial permit expires on the first birthday of the applicant occurring after the fourth anniversary of the date it was issued). You must be a minimum of 21 years of age, the cost is $140, and the processing time is 60-180 days. Under Texas' Public Information Act state officials are allowed to confirm the names of individual concealed carry permit holders. Nomads that demand the ability to legally carry a concealed weapon may find Texas a more appropriate state for domicile.

State Income Tax: None

I have assisted clients with nomad registration through both Texas and South Dakota. Both are fine options. South Dakota will be a bit easier overall, but requires you to visit the state on occasion. Texas may require annual visits, but that could be a more pleasant experience. The process is very similar with both states, and I will explain every detail of each. Let's start with South Dakota.

The first step is to gather all of your documentation from your PMB provider. If you chose Escapees, collect your receipt for your PMB and the documentation acknowledging your PMB address. Make sure that you selected the South Dakota option during your registration and ensure you were issued a South Dakota PMB. Hopefully, you have already changed your address with your bank, and you have a monthly statement (either digital or mailed) that displays this new address. Have a copy of this statement. Overall, you want at least two pieces of documentation that confirm your name and PMB address.

Next is the biggest step. It is time to go to South Dakota. Make sure you spend the night upon arrival at a hotel in Pennington County, the county of your PMB address. When you check out of the hotel, be sure to obtain a receipt from your stay, and ensure that your name and PMB address appear on the receipt. If your spouse, partner, or family member is also becoming a nomad, make sure they each have their own receipt with this same information. I have found most hotels will edit the name and address on the receipt any way you wish. They are very familiar with this process.

Next, visit the department of motor vehicles (DMV) in Rapid City. You can make an appointment online which may prevent long waits. In my experience, there is rarely much of a crowd. Explain that you are there to obtain a driver's license as a nomad. They will know what this means and the scrutiny will begin.

Have your hotel receipt, previous unexpired driver's license, and second form of identification ready. This can be a passport or certified birth certificate (I would bring both). Also, have either your original Social Security card or a 1099 tax form stating your name and SSN. Have a Residency Affidavit printed and completed. At the time of this writing, a copy can be found at https://dps.sd.gov/application/files/2815/1085/4078/ResidencyAffidavit.pdf.

The following page displays this document. The content in brackets, ([ ) and ( ]), displays explanations about each section. I have assisted numerous people with this entire process. In each scenario, we walked out of the DMV with a new South Dakota Driver's License less than 20 minutes after entering. The only issue I have had was with a newly married couple. The wife possessed a birth certificate and passport in her maiden name and a license in her married name. This is acceptable, but you must provide a marriage certificate along with the other documents. Fortunately, we were able to obtain the document later that afternoon.

RESIDENCY AFFIDAVIT
FOR SOUTH DAKOTA RESIDENTS WHO TRAVEL
AND DO NOT HAVE A RESIDENCE IN ANOTHER STATE

The purpose of the following questions is to determine if you meet the qualifications for an exception of the proof of residency requirements for obtaining a South Dakota Driver License or non-driver ID card.

This form must be signed by a notary of the public or a South Dakota driver license examiner.

[This can be notarized at the DMV.]

1. Is South Dakota your state of residence? _____Yes _____No

[You must select Yes in order to qualify. Since you possess a PMB, that is the technical requirement to declare residency, along with surrendering your previous license.]

2. Is South Dakota the state you intend to return to after being absent? _____ Yes _____No

[Again, you must select Yes to qualify. This assumes you will be traveling, will not be physically present within the state, but will return at some point.]

This form must be accompanied by a valid one-night stay receipt (no more than one year old) from a local RV Park, Campground, or Motel for proof of the temporary address where you are residing. In addition, you must submit a document (no more than one year old) proving your personal mailbox (PMB) service address (receipt from the PMB business or a piece of mail with your PMB address on it).

PLEASE NOTE: South Dakota Driver Licensing records are used as a supplemental list for jury duty selection. Obtaining a South Dakota driver license or non-driver ID card will result in you being required to report for jury duty in South Dakota if selected.

[In my experience, your chances of being called for jury duty are minimal. If you do get the call, contacting the court and explaining that you do not physically live in South Dakota will dismiss your obligation.]

I declare and affirm under the penalties of perjury (2 years imprisonment and $4000 fine) that this claim (petition, application, information) has been examined by me and, to the best of my knowledge and belief, is in all things true and correct. Any false statement or concealment of any material facts subjects any license or ID issued to immediate cancellation.

This is a major accomplishment. You now have a new license in a state which you do not live in permanently. The address on the license is a mail drop that you have never visited. Within months, this address will be listed as your official residence at the credit bureaus, data mining companies, and other entities that monitor all of us. Surprisingly, this is still legal. By declaring yourself a nomad, and the generosity of South Dakota in becoming your domicile, you are now officially a resident of the state. You have given up the residency provided by your previous state. Don't take that lightly, and consider these actions before executing.

Residency and domicile are two distinct terms, but often used interchangeably. This adds to the confusion when trying to decide if you are legally a "resident" of a state. A person may be a resident of multiple states, but is usually only domiciled in one state. A person may own homes in several states and spend time in each of those homes during the year, but only one state will be their domicile. As a general rule, the state where you are domiciled will be the state where you live (at least part of the year), work, receive mail, conduct banking, and register and insure your vehicles.

You establish domicile when you are a resident of a state and intend to make that state your home. While you may not have a mortgage or lease in the state that you choose as a domicile, you can connect your life to that state. In other words, the more of a connection that you have with a particular state, and the less of a connection you maintain with any other state, the more likely it is that your claims to be domiciled there will hold up if ever called into question.

Overall, if your driver's license, mailing address, and other official documentation are in the state of your chosen domicile, you are a resident of that state. Once your license is obtained, you should identify all other official accounts and services in your name and update the physical address on file. This was mentioned in a previous chapter, but it is worth repeating. Your bank accounts, investment services, credit cards, passport, and anything else you can think of can now possess your new PMB address. If any service gives you grief, you have a government identification card to show them that matches your new information. Before we move on to Texas, there are a few more caveats that I have experienced.

- The South Dakota driver's license qualifies under the Real ID Act. This means your license will have the "gold star" which is accepted as identification by the TSA at airports.
- While you are at the DMV, request a standard identification card. This is similar to a license, but can only be used as traditional identification. Store this in a safe place. It can be helpful if you lose your license, and must wait for a new duplicate copy.
- South Dakota allows you to renew your license online after your initial five years has expired. However, you are still required to be present within the state for at least one night within a year prior to the renewal date.

The process for Texas is similar with a few noticeable changes and annoyances. The first step is to secure your Texas PMB address as outlined previously. Hopefully, you have already started updating your address to the PMB and are beginning to receive mail in your name. Similar to South Dakota, you will need to be physically present at the Department of Public Safety office in Texas to complete the domicile process. You must provide a valid and unexpired driver's license, and surrender it when applying for the new license. You will complete the application while at the Department of Public Safety office. There are many unique considerations if choosing Texas as a domicile.

You will be required to present one additional primary identity document, such as a passport. If that is not available, you will need three secondary identity documents such as a certified copy of birth certificate, Social Security card, 1099 tax form, or a passport card. I always suggest taking all possible identification you own.

You will also be required to register your vehicle at this time. South Dakota is much more lenient with vehicle registration, and that process will be discussed in the upcoming Private Vehicles chapter. Since Texas demands this to happen right away, let's tackle the details.

A vehicle owner has 30 days to register a vehicle after establishing residency (PMB) in Texas. The vehicle has to be physically present in Texas to be inspected, and you will be given a Vehicle Inspection Report (VIR). You will need to obtain your own inspection in Texas and provide proof to the county tax office along with the proof of insurance.

Vehicle owners who are still making payments on their vehicle will need to complete Texas Certificate of Title (Form 130-U), the Application for Registration Purposes Only (Form VTR-272), and provide current proof of registration. All forms are available at https://www.txdmv.gov/forms-tac. Vehicle owners who are no longer making payments on their vehicle will need to produce the current title and current registration.

The next vital piece is the Texas Residency Affidavit. You can find a blank copy of this online at http://www.dps.texas.gov/internetforms/forms/dl-5.pdf, and the DMV should also have copies. I always prefer to have a completed version when I arrive. The following page is a replica of the affidavit.

Texas Residency Affidavit

Instructions for completion are on back of form

To be eligible for a Texas driver license or identification card, the applicant must be a resident of or domiciled in Texas. If the applicant cannot provide two acceptable residency documents from the list found on the back of this form, this affidavit may be used as evidence of residency in Texas.

*Texas domicile rules are in the Texas Administrative Code (37 TAC §§ 15.49 and 16.15).

The applicant for a Texas driver license or identification card must complete Section A.

A. Applicant Information

Name _____

Residence Address _____ City _____ State _____ ZIP Code _____

I certify that the information provided above is true and correct. I understand that according to Texas law, it is a crime to knowingly make any false statement relating to the application for a driver license or identification card.

Applicant's Signature _____ Date _____

Notary:

The details provided on this form should be your Texas PMB. Be sure to have the following documentation along with this affidavit.

- Receipt from Escapees for your PMB, including the Texas address and date acquired
- A piece of mail sent to your PMB in your name, such as a bank statement
- A second piece of mail, such as a credit card statement, mailed to you at the PMB
- Receipt from a recent hotel stay in Texas, addressed to you at your PMB address

As you can see, there are a few additional complications when choosing Texas as your state for domicile. These may be justified for your situation. In my experience, the DMV employees in South Dakota are much more prepared for your nomad declaration, and more helpful. In Texas, I have found employees who had no idea how to proceed, and supervisors who seemed uneducated in the process. I have experienced denials in Texas because new documentation requirements were in effect which were not publicly posted. Overall, my attempts in South Dakota have been much smoother.

Renewals

In the previous state summaries, I explained that both Texas and South Dakota allow one remote renewal every ten years. This means that your first renewal, after five years in South Dakota, can be completed online. However, the official instructions on the state website are not complete. The following explains the exact process, using South Dakota as an example.

Approximately six months before your license expires, you should receive a postcard from the state notifying you that your expiration date is coming soon. It will include the URL to the state DMV website, which was https://dps.sd.gov/driver-licensing/renew-and-duplicate at the time of this writing. From there, you can choose the "Am I Eligible" button and enter your driver's license number. Most nomads should qualify for online renewal. You will be asked a series of questions, which are likely identical to the questions answered during your original application. You must pay the processing fee during this renewal process via credit card, which should be under $30. Be sure to provide a valid email address. Once you complete the process, you wait.

Approximately one week after submission, you should receive an email from the DMV stating that your application is incomplete. Since you are a nomad, you are required to sign a new Nomad Affidavit form and submit proof on one night's stay in South Dakota within the previous year. The form will be included, and must be notarized, the same as before. Your proof of being within the state over the past year can vary. I usually submit a hotel receipt in the name of my client. You can email scans of these documents by responding to the message. This brings up an important consideration. When should you revisit the state?

You could always travel to South Dakota within six months of your license expiration, but that timing may not be optimal. Cold weather and other plans could get in the way. I encourage clients to schedule a brief trip within one year of expiration around their schedule. This could be during a planned road trip or downtime between other travel. What is important is that you plan accordingly and do not find yourself about to expire while nowhere near the state. If you travel to South Dakota before your renewal eligibility period, simply keep a receipt as proof. You can submit it later once you are allowed to renew. I prefer to go in summer months, but your preference may vary.

Two weeks after the email submission, you should receive your new driver's license at your PMB. It will contain the same photo as the previous version. When this license expires, you must travel to South Dakota and obtain a new version in person. With this plan, you only need to be within the state twice every ten years.

Regardless of which state you choose, always contact the DMV before you plan your trip. Confirm that you have everything they demand in order to establish residency. It is quite a setback to show up without a mandatory piece of information and be told to come back after you have everything required. Be overly prepared.

Taxes

As another benefit, these states do not collect any state earnings tax from their residents. This also applies to travelers who use these states as a permanent address. Before you decide that you can live in a state that taxes income while becoming exempt in a state that does not, think again. It simply does not work like that. Consider the following scenarios.

You are a nomad with domicile in South Dakota. You are traveling the country and spend some time in Illinois. You pick up a job and receive payment via check. Your employer withholds state taxes for Illinois. You will be required to file annual Illinois state taxes regardless of your "home" address.

You are a nomad with domicile in Texas. You are self-employed. You spend the majority of your time in New York and rent an apartment. You are required to pay your share of New York income tax. You would need to file an annual New York state return.

Many readers may think they can avoid this and will roll the dice. This is a mistake. One of the most invasive privacy violations is a tax audit. Play by the rules, pay your appropriate state taxes, consult an accountant, and stay off their radar. Federal taxes to the IRS are not impacted by a nomad residency. You would pay these as with any other residency situation. Do not violate any tax laws.

Voting

Both Texas and South Dakota can register you to vote at the time of obtaining a driver's license. You will then be allowed to vote remotely via nominee without entering the state on federal elections. I won't spend much time discussing the details of this, as I no longer recommend that my clients register to vote. This has nothing to do with patriotism or a duty to vote as an American. It is simply because it is impossible to protect your voter registration details from public view. Voter details are public and released in mass quantities to political entities and private companies. If you are registered to vote, your name, DOB, and PMB

address are now public information. If you prefer to keep that private, be sure to tell the DMV that you do not wish to register to vote at this time.

Establishing yourself as a domiciled nomad is a big decision which warrants some serious thought. Once complete, you possess a driver's license in a state that does not demand your presence, and displays a physical address you may have never visited. These details will become tightly associated with your identity. When an adversary starts hunting for you, the first and most logical place to find you will be an address shared by thousands of people. This will be a dead lead. This single tactic may be all you need to prevent your next home address from becoming public information.

Health Insurance

If you are unemployed or self-employed, it is very likely you are responsible for your own health insurance coverage. The Affordable Care Act (ACA) previously required everyone to possess health insurance, and charged a fee to those who could afford it but chose to go without it. In 2019, this fee was repealed, and the IRS no longer mandates a financial penalty from those with no coverage. This book was written in 2020, and things could be different by the time you read this. As of now, health insurance is technically still required for all of us, but there seems to be no enforcement of this. Regardless of your opinion of the ACA, you should still explore your options for health coverage as a nomad.

Overall, U.S. citizens who have no health coverage through an employer or other avenue acquire their own health insurance through the marketplace of their domicile state. Both South Dakota and Texas use the federal exchange, and residents enroll through the official HealthCare.gov website. Currently, South Dakota offers two providers while Texas offers eight. For traditional coverage, you would enroll at HealthCare.gov and learn about your options. Many of my clients do not go this route.

My wealthy clients often choose high-deductible plans in order to meet specific state and federal requirements while paying lower monthly premiums. If they need to see a doctor or visit a hospital, they pay out-of-pocket until the deductible is met. I have seen this be as high as $10,000 annually. This works well for them because they have the money to pay for services as needed, and only desire coverage for major catastrophes such as an automobile accident or diagnosis of cancer. Clients who cannot afford high monthly premiums also seek out these types of plans, and hope to stay healthy.

Some clients have elected healthcare sharing plans which are not technically health insurance, but pay medical bills when necessary. Many of these qualify for an exemption from the ACA. The most popular of these is Medi-Share. The premiums are very low and coverage has no financial limit. However, there is a catch. Medi-Share is a Christian-based organization, and as

a private company they are allowed to apply any restrictions desired. As a small example, they do not provide any coverage, or "sharing", for abortions, unwed pregnancies, birth control, substance abuse treatment, alcohol-related crashes, and many other scenarios which they believe conflict with their beliefs. For many people, this option would never be considered because of these restrictions. For others, it is acceptable.

I leave you with my thoughts on healthcare coverage. I believe you should have a solution in mind before considering the nomad lifestyle. These are not easy decisions which should be made hastily. Once you decide on the coverage appropriate for you, contact a provider and make sure they will work with your nomad plans. Possessing no coverage can leave you in a permanent negative financial situation. Purchasing the common default state coverage may leave you with high premiums from which you never benefit. Explore all of your options, and research ideas outside of HealthCare.gov. Any provider will demand your full name, DOB, and SSN, but all should accept your PMB address as "home".

Summary

Possessing a PMB address as your official "home" address on your driver's license has many advantages. You now have an address which can be given out freely without jeopardizing your privacy. You can share this address with banks, lenders, government entities, and private institutions, all without disclosing your actual home location. You can be legally domiciled in a state which respects your right to travel and not be present within the state. Traditionally, your state domicile demands on knowing, and sharing, your true home address. This results in your home address eventually appearing within public people search websites. When your PMB address leaks online, the damage is minimal. No one will ever find you at that address. You can possess a permanent mailing address regardless of your future travel plans and living situations. You can drive anywhere in the country while obeying all registration laws. Having a PMB and nomad residency will assist with many of the upcoming privacy strategies. However, please note that nomad residency is not required in order to apply the techniques within the remainder of this book.

Nomad Residency is appropriate for my clients which face an immediate physical threat and must relocate. It provides a legal domicile while the client takes some time to figure out the future. It is not appropriate for those employed within another state with close community ties toward a specific area. Many clients choose this path while executing retirement plans or after leaving a career. I have many friends in the military which use this strategy while being deployed. There are many reasons to embrace nomad residency and equally as many reasons to avoid it. Choose wisely. Consider one final situation a client faced in 2018.

This person executed complete nomad residency through Texas. He went through every step you read in this chapter. He possessed a Texas DL and registered his vehicle in the state. He then reached out to me about purchasing an anonymous home within the name of a trust in California.

He had no intention of traveling much and would call California his home. I advised that this would create many complications because he would then be legally required to declare California his domicile state, and would lose his privacy protection. He understood, and said he would take his chances. He was retired and believed that California would never know he was living in the state. I declined my services unless he agreed to obey all state laws once he purchased the house. He proceeded without me and purchased a home in a trust.

Nine months later, he received an intimidating letter from the state of California. Some of the thousands of license plate readers throughout the state captured his Texas vehicle plates on a consistent basis within a specific city (where he lived). The state demanded that he register himself and his vehicle within the state, and file state income taxes with the Franchise Tax Board (FTB). This stern warning outlined the extensive fines if he did not comply. California does not mess around with non-residents living inside its boundaries. He complied, registered under his home address, and his name now appears on many people search websites with all of the details.

You can absolutely purchase an "invisible" home in the name of a trust in aggressive states such as California, and possess a great layer of privacy. However, when doing so you must become an official resident of the state and comply with all laws. You can file state income taxes to the address of a PO Box, and display a PO Box on your DL in some locations, but the state will demand to know your true residence. I do not accept new clients who insist on living in California full-time while declaring themselves a nomad in another state. It will catch up to them. Aggressive states such as California and New York employ many investigators looking for this activity in order to collect as much revenue as possible. I share this as a warning to readers thinking they can bend the rules while staying anonymous.

Before considering nomad residency for your needs, be sure you completely understand the state laws of BOTH the nomad state and the state where you will be spending much of your time. This method is not intended to be used to avoid a specific state's politics or government requirements. It is a valid strategy for those willing to travel enough to obey the rules of being a nomad. My clients who became legal nomads travel the world, follow great weather, and experience a life which most of us may find unstable at times. They obey the rules to which they agreed with the state of their choice and are sure to not violate any residency requirements of non-nomad states. When properly and legally executed, it offers a level of privacy unavailable within any other tactic.

International Considerations: This chapter was heavily focused on citizens of America. Many other countries also offer some level of nomad registration. However, the term "nomad" may not be applicable to situations similar to those described in this chapter. I encourage international readers to explore the options available in their own countries of residence. I have received the most beneficial information by contacting local homeless shelters and questioning the ways in which people without physical addresses legally comply with government mandates.

Chapter Five

Legal Infrastructure

If you ever plan to own any assets such as a home or vehicle, you will need some type of legal infrastructure in order to keep it private. This is a holding device which technically owns the asset. Even if you only plan to rent your housing for the rest of your life, you will need to obtain utilities and services which traditionally require your real name. Legal entities such as Limited Liability Companies (LLCs) and Trusts can provide a valuable layer of privacy between you and the asset. This chapter outlines specific types of legal infrastructures that you may need in order to complete the rest of this book. None are expensive, and some are free. Before I can proceed with anything, please consider the following paragraph very carefully.

I am not an attorney. I am not YOUR attorney. You should not replicate anything I discuss in this chapter without first consulting an attorney. The following is not legal advice. It is not any type of advice. It is merely explicit examples of the actions I have taken to create legal entities for myself and clients. This chapter is not intended to be a complete representation of the many complexities of trusts and LLCs. It is overly simplified in order to only focus on the issues important for privacy protection. Nothing in this chapter is meant for business use or income. Your scenario will be unique from mine and your privacy plan will require modification from mine. Seek professional legal advice.

Let's start with a trust. There are many types of trusts and you may have heard of a living trust, land trust, or property trust. These are all fairly similar with various levels of complication attached to each. Overall, a trust is a legal entity that you can create at any time. It can be as simple as a few pieces of paper written as a contract. You can't see a trust, or touch it, but it does exist. The first step in creating a working trust is to prepare and sign a document called a "Declaration of Trust".

Once you create and sign the Declaration of Trust, the trust exists. There must be a person in charge of this trust, who is called the "trustee". With traditional trusts, the trustee manages the property on behalf of someone else, called the "beneficiary", which could be you. However, with a living trust, you are usually the trustee and beneficiary of the trust until you die. Only after your death do the trust beneficiaries you've named in the Declaration of Trust have any rights to your trust property. This may sound complicated, but it does not need to be. Let's walk through each step of creating a living trust first, as it is usually the most familiar to people.

Living trusts are an efficient and effective way to transfer property to relatives, friends, or entities at your death. Essentially, a living trust performs the same function as a will, with one big difference. The assets left by a will must go through the probate court process. In probate, a deceased person's will must be proven valid in court, then the person's debts are paid, and finally the remaining property is distributed to the beneficiaries. This can take over a year. These probate court proceedings waste time and money. By contrast, assets left by a living trust can go directly to your inheritors. They do not need to bother with a probate court proceeding. That means your beneficiaries will not need to spend any of your money to pay for court and lawyer fees. More importantly, the details of the trust are private. If you truly value your privacy, you may want to have one last strategy in place that keeps your final wishes a secret from the public.

All transactions that are associated with your living trust are reported on your personal income tax return. You do not need a separate tax identifier and a trust is not considered a business in the eyes of the law. These trusts are called "living" because they are created while you are alive. They are called "revocable" because you can revoke or change them at any time until you die. While you are alive, you maintain ownership of all property that you transferred to your living trust. You can do whatever you wish with your trust property, including selling it or giving it away. If you want, you can terminate the entire trust as if it never happened (unless you have assets already titled within the trust). A revocable living trust becomes permanent at your death. Then, it allows your trust property to be privately transferred to the people or organizations you have named as beneficiaries of the trust.

For the record, I do NOT recommend titling your home in a LIVING trust. The first reason is that the beneficiary of a living trust is typically also the trustee. This will likely make your name publicly associated with the home. Second, I never recommend titling a home in the same trust as other assets. However, a living trust still has a place in the private person's arsenal. It is a great means to hold investment accounts, online savings accounts, certificates of deposits, vehicles, and other physical items. Let's first learn the basic elements inside of a living trust. After, I will explain a traditional trust which takes things a step further.

First, you need a name for the living trust. The customary option is to title the trust to include your name, such as The Bazzell Family Trust. I disagree with this, and I encourage you to select a more common and generic name. The name you choose can be used on other trusts by other people, it does not need to be unique. As an example, you may choose The Financial Planning Living Trust or the 45886 Living Trust. Keeping your name off the title gives you a bit of privacy when it is publicly released as the owner of an asset. Next, it is time to create the Declaration of Trust, which is essentially the contract that makes the living trust valid. The following pages outline a typical living trust template, with an explanation of each section within brackets ([ ) and ( ]).

The Financial Planning Living Trust
Declaration of Trust

I. Trust Name

This trust shall be known as The Financial Planning Living Trust. It is a REVOCABLE trust created on January 1, 2019.

[This simply identifies the name of the trust and the date it was established. This name and date combination assist with identification and will need to always be accurate as you add assets into the trust. It also clearly defines this trust as revocable by you.]

II. Trust Property

(A) Property Placed in Trust

[YOUR NAME], called the grantor or trustee, declares that he has set aside and holds in The Financial Planning Living Trust all of his interest in that property described in the attached Schedule A. The trust property shall be used for the benefit of the trust beneficiaries and shall be administered and distributed by the trustee in accordance with this Declaration of Trust.

[This section identifies you as the grantor and trustee of this living trust. This gives you all of the power to manage the trust.]

(B) Additional or After-Acquired Property

The grantor may add property to the trust at any time.

[This allows you to place any future assets into the trust.]

III. Reserved Powers of Grantor

(A) Amendment or Revocation

The grantor reserves the power to amend or revoke this trust at any time during his lifetime, without notifying any beneficiary.

[This allows you to change or completely terminate the trust at any time.]

(B) Rights to Trust Property

Until the death of the grantor, all rights to all income, profits, and control of the trust property shall be retained by the grantor.

[This ensures you have the right to do anything you like with the trust until you die.]

(C) Homestead Rights

If the Grantor's principal residence is held in this trust, Grantor has the right to possess and occupy it for life, rent-free and without charge, except for taxes, insurance, maintenance, and related costs and expenses. This right is intended to give Grantor a beneficial interest in the property and to ensure that Grantor does not lose eligibility for a state homestead tax exemption for which Grantor otherwise qualifies.

[If you decide to title a home in the living trust, this ensures you have the right to live in the home.]

(D) Grantor's Death

After the death of the grantor, this trust becomes irrevocable. It may not be altered or amended in any respect, and may not be terminated except through distributions permitted by this Declaration of Trust.

[Living trusts are locked in when the grantor dies. This ensures your desires upon death are met.]

IV. Trustees

(A) Original Trustee

The trustee of The Financial Planning Living Trust shall be [YOUR NAME] of [YOUR CITY], [YOUR COUNTY], [YOUR STATE], Date of Birth [YOUR DOB], SSN [YOUR SSN].

[This identifies you as the trustee of the trust. These details are private because this trust is never filed publicly. During the next trust option, you will learn how to assign another trustee.]

(B) Successor Trustee

Upon the death of the trustee, or his incapacity, the successor trustee shall be [NAME] of [CITY], [COUNTY], [STATE], Date of Birth [DOB], SSN [SSN]. If he is deceased or unable to serve or continue serving as successor trustee, the successor trustee shall be [NAME] of [CITY], [COUNTY], [STATE], Date of Birth [DOB], SSN [SSN].

[This identifies the person you wish to administer the trust upon your death. The second name is the backup in the event that your first choice is also deceased. These should be people who you are confident will honor the rules of the trust.]

(C) Trustee's Responsibility

The trustee in office shall serve as trustee of all trusts created under this Declaration of Trust.

[This declares the power issued to you as trustee of your own living trust.]

(D) Terminology

In this Declaration of Trust, the term "trustee" includes any successor trustee or successor trustees.

[This defines terminology for the trust to apply to your successor trustee in the case of your death.]

(E) Bond Waived

No bond shall be required of any trustee.

[Legal speak to state that a bond or insurance is not required.]

(F) Compensation

No trustee shall receive any compensation for serving as trustee.

[This declares that trustees are not paid for services.]

(G) Liability of Trustee

With respect to the exercise or non-exercise of discretionary powers granted by this Declaration of Trust, the trustee shall not be liable for actions taken in good faith.

[This protects the trustee.]

V. Beneficiaries

Upon the death of the grantor, the property of The Financial Planning Living Trust shall be distributed to the beneficiaries named in this section.

[This is where you declare the people who should receive your assets when you die.]

(A) Primary Beneficiary

[NAME] shall be given all [YOUR NAME]'s interest in the property listed on Schedule A. If [NAME] does not survive the grantor by thirty (30) days, that property shall be given to the alternative beneficiaries.

[This allows you to give all of your assets within the trust to a single person, such as a spouse.]

(B) Alternative Beneficiary

The following property shall be given to the identified alternative beneficiaries ONLY if [NAME] does not survive the grantor by thirty (30 days).

[This allows you to specify the people that should receive your assets when you die if the primary beneficiary has also deceased. The following is one example.]

The grantor's children, [NAME], [NAME], [NAME], and [NAME], shall be given all financial accounts and assets listed in Schedule A in the following shares:

25% to [NAME]
25% to [NAME]
25% to [NAME]
25% to [NAME]

If any alternative beneficiaries do not survive the grantor by thirty (30) days, those shares shall go to the remaining alternative beneficiaries, in equal shares.

[This specifies that the remaining people alive receive equal shares of the trust if an alternative beneficiary has deceased.]

(C) Residuary Beneficiary

The residuary beneficiary of the trust shall be [NAME]. If [NAME] does not survive the grantor by thirty (30) days, any and all property shall be given to the alternative beneficiaries in the shares specified in Section V, Paragraph (B).

[This is a "catch-all" that specifies any leftover assets go to a single person.]

VI. Distribution of Trust Property Upon Death of Grantor

Upon the death of the grantor, the trustee shall distribute the trust property outright to the beneficiaries named in Section V, Paragraphs (A), (B) and (C).

[This instructs the trustee to distribute the assets as you outlined.]

VII. Trustee's Powers and Duties

(A) Powers Under State Law

To carry out the provisions of The Financial Planning Living Trust, the trustee shall have all authority and powers allowed or conferred on a trustee under [STATE] law, subject to the trustee's fiduciary duty to the grantor and the beneficiaries.

[This identifies the state laws that should be used when identifying the powers of the trust. This is usually your state of residence or domicile.]

(B) Specified Powers

The trustee's powers include, but are not limited to:

1. The power to sell trust property, and to borrow money and to encumber that property, specifically including trust real estate, by mortgage, deed of trust, or other method.
2. The power to manage trust real estate as if the trustee were the absolute owner of it, including the power to lease (even if the lease term may extend beyond the period of any trust) or grant options to lease the property, to make repairs or alterations, and to insure against loss.
3. The power to sell or grant options for the sale or exchange of any trust property, including stocks, bonds, debentures, and any other form of security or security account, at public or private sale for cash or on credit.
4. The power to invest trust property in property of any kind, including but not limited to bonds, debentures, notes, mortgages, stocks, stock options, stock futures, and buying on margin.
5. The power to receive additional property from any source and add to any trust created by this Declaration of Trust.
6. The power to employ and pay reasonable fees to accountants, lawyers, or investment experts for information or advice relating to the trust.
7. The power to deposit and hold trust funds in both interest-bearing and non-interest-bearing accounts.
8. The power to deposit funds in bank or other accounts uninsured by FDIC coverage.
9. The power to enter into electronic fund transfer or safe deposit arrangements with financial institutions.

10. The power to continue any business of the grantor.
11. The power to institute or defend legal actions concerning the trust or grantor's affairs.
12. The power to diversify investments, including authority to decide that some or all of the trust property need not produce income.

[This section specifies the powers granted to the trustee. These allow the trustee to legally execute various requirements of the trust.]

(C) Payment by Trustee of the Grantor's Debts and Taxes

The grantor's debts and death taxes shall be paid by the trustee however he deems appropriate.

[This allows the trustee to pay off your debt and taxes from the trust if desired.]

VIII. General Administrative Provisions

(A) Controlling Law

The validity of The Financial Planning Living Trust shall be governed by the laws of [STATE].

(B) Severability

If any provision of this Declaration of Trust is ruled unenforceable, the remaining provisions shall nevertheless remain in effect.

(C) Amendments

The term "Declaration of Trust" includes any provisions added by amendments.

(D) Accountings

No accountings or reports shall be required of the trustee.

[These are a few final formalities that finish the trust's legal requirements.]

Certification by Grantor

I certify that I have read this Declaration of Trust for The Financial Planning Living Trust, created January 1, 2019, and that it correctly states the terms and conditions under which the trust property is to be held, managed, and disposed of by the trustee, and I approve the Declaration of Trust.

Dated: January 1, 2019

_____

Grantor and Trustee – [YOUR NAME]

[This is your signature attesting the creation of this trust. This document should be notarized. I prefer to keep this page separate from the rest of the trust in case an entity requires the page including your signature to be kept on file.]

(New page)

Schedule A

All the grantor's interest in the following property:

ANY ACCOUNTS PLACED INTO THE TRUST

[This would include any assets or properties that you obtain in the name of the trust. You can also include physical items, such as collectibles, but cannot include cash.]

The previous living trust was an example of a document commonly created by those desiring asset protections when they die. It is often associated with elderly people planning for their death and wanting to keep their assets out of probate. This can save a lot of money for their beneficiaries since a probate judge does not need to decide whether a will is valid. This document alone really means nothing until you place assets into the trust. Most people re-title their home into the trust and add all of their financial accounts. When the grantor dies, all of the assets within the trust on Schedule A instantly remain property of the trust. The successor trustee now has the power to distribute the assets in the trust to the beneficiaries defined in the document. This is why choosing a trustworthy successor trustee is vital.

Before you establish your own living trust, think about how it will be used. As stated previously, I usually do not advise the use of a LIVING trust, with you as the trustee, for a home purchase. Your name will likely be filed at the county level in connection with the home and you lose all privacy. I also do not recommend placing your home into the same trust that holds assets in financial accounts. This would connect you and your SSN with the house. Therefore, I only recommend a living trust to privacy enthusiasts if it will be used for financial accounts, such as your investments and online banks. You can title these accounts into the name of your living trust, and the accounts can be distributed by your successor trustee upon your death. There will be no probate, court hearings, or delays. Most importantly, the details of this trust will never be made public. You should contact your financial account companies and request details on transferring your accounts to the living trust.

There are some assets that should not be placed into a living trust. These include tax-deferred retirement accounts such as 401Ks and personal checking accounts that are already set up as "Payable on Death". Traditionally, the living trust is mostly used for homes and other valuable assets by those that do not require extreme privacy. Most people that place their home into a living trust have no concern publicly associating the trust with their real name. It is simply to avoid the probate process involved with typical wills. As a privacy enthusiast, you should consider other options for trusts.

Specifically, you may want to avoid any definition within the trust name. Adding "Living Trust" to the title of the trust gives it an association to a document that you created in preparation for death. Adding "Land Trust" identifies the purpose as to hold real estate. Adding "Property Trust" indicates it will only be used to hold a specific asset. I propose eliminating this behavior, and only referring to your trust as a "Trust", such as The XYZ Trust. Many state trust laws do not acknowledge a difference between various types of trusts. Some state laws apply very specific (and undesired) rules when you label a trust as a Land Trust, which no longer take advantage of the simplification of a traditional trust. Consider the following trust example. It will appear very similar to the previous example, and I will only include an additional explanation within brackets when there is a change.

The XYZ Trust
Declaration of Trust

I. Trust Name

This trust shall be known as The XYZ Trust. It is a REVOCABLE trust created on January 1, 2019.

II. Trust Property

(A) Property Placed in Trust

[NAME], the Grantor, declares that he has set aside and holds in The XYZ Trust all of his interest in that property described in the attached Schedule A. The trust property shall be used for the benefit of the trust beneficiaries and shall be administered and distributed by the Trustee in accordance with this Declaration of Trust.

[This identifies you as the grantor only, which gives you the power of this trust.]

(B) Additional or After-Acquired Property

The Grantor may add property to the trust at any time.

III. Reserved Powers of Grantor

(A) Amendment or Revocation

The Grantor reserves the power to amend or revoke this trust at any time during his lifetime, without notifying any beneficiary.

(B) Rights to Trust Property

Until the death of the Grantor, all rights to all income, profits, and control of the trust property shall be retained by the Grantor.

(C) Homestead Rights

If the Grantor's principal residence is held in this trust, Grantor has the right to possess and occupy it for life, rent-free and without charge, except for taxes, insurance, maintenance, and related costs and expenses. This right is intended to give Grantor a beneficial interest in the property and to ensure that Grantor does not lose eligibility for a state homestead tax exemption for which Grantor otherwise qualifies.

(D) Grantor's Death

After the death of the Grantor, this trust becomes irrevocable. It may not be altered or amended in any respect, and may not be terminated except through distributions permitted by this Declaration of Trust.

IV. Trustees

(A) Original Trustee

The Trustee of The XYZ Trust shall be [NAME] of [CITY], [COUNTY], [STATE], Date of Birth [DOB], SSN [SSN].

[This is the major deviation of this trust versus the living trust. Here, you assign someone else as the trustee. This name will be publicly associated with the trust if you purchase a home, and we will dive into that aspect in a following chapter.]

(B) Successor Trustee

Upon the death of the trustee, or his incapacity, the successor trustee shall be [NAME] of [CITY], [COUNTY], [STATE], Date of Birth [DOB], SSN [SSN]. If he is deceased or unable to serve or continue serving as successor trustee, the successor trustee shall be [NAME] of [CITY], [COUNTY], [STATE], Date of Birth [DOB], SSN [SSN].

[This should be people which you trust to handle affairs associated with the trust. There will be much more discussion about this later.]

(C) Trustee's Responsibility

The Trustee shall serve as Trustee of all trusts created under this Declaration of Trust.

(D) Terminology

In this Declaration of Trust, the term "Trustee" includes any successor Trustee or successor Trustees.

(E) Bond Waived

No bond shall be required of any Trustee.

(F) Compensation

No Trustee shall receive any compensation for serving as Trustee.

(G) Liability of Trustee

With respect to the exercise or non-exercise of discretionary powers granted by this Declaration of Trust, the Trustee shall not be liable for actions taken in good faith.

V. Beneficiaries

Upon the death of the Grantor, the property of The XYZ Trust shall be distributed to the beneficiaries named in this section.

(A) Primary Beneficiary

[NAME] shall be given all [YOUR NAME]'s interest in the property listed on Schedule A. If [NAME] does not survive the grantor by thirty (30) days, that property shall be given to the alternative beneficiaries.

(B} Alternative Beneficiary

The following property shall be given to the identified alternative beneficiaries ONLY if [NAME] does not survive the grantor by thirty (30 days).

The grantor's children, [NAME], [NAME], [NAME], and [NAME], shall be given all financial accounts and assets listed in Schedule A in the following shares:

25% to [NAME]
25% to [NAME]
25% to [NAME]
25% to [NAME]

If any alternative beneficiaries do not survive the grantor by thirty (30) days, those shares shall go to the remaining alternative beneficiaries, in equal shares.

(C) Residuary Beneficiary

The residuary beneficiary of the trust shall be [NAME]. If [NAME] does not survive the grantor by thirty (30) days, any and all property shall be given to the alternative beneficiaries in the shares specified in Section V, Paragraph (B).

VI. Distribution of Trust Property Upon Death of Grantor

Upon the death of the Grantor, the Trustee shall distribute the trust property outright to the beneficiaries named in Section V, Paragraphs (A), (B) and (C).

VII. Trustee's Powers and Duties

(A) Powers Under State Law

To carry out the provisions of The XYZ Trust, the Trustee shall have all authority and powers allowed or conferred on a Trustee under [STATE] law, subject to the Trustee's fiduciary duty to the Grantor and the beneficiaries.

(B) Specified Powers

The Trustee's powers include, but are not limited to:

1. The power to sell trust property, and to borrow money and to encumber that property, specifically including trust real estate, by mortgage, deed of trust, or other method.

2. The power to manage trust real estate as if the Trustee were the absolute owner of it, including the power to lease (even if the lease term may extend beyond the period of any trust) or grant options to lease the property, to make repairs or alterations, and to insure against loss.

3. The power to sell or grant options for the sale or exchange of any trust property, including stocks, bonds, debentures, and any other form of security or security account, at public or private sale for cash or on credit.

4. The power to invest trust property in property of any kind, including but not limited to bonds, debentures, notes, mortgages, stocks, stock options, stock futures, and buying on margin.

5. The power to receive additional property from any source and add to any trust created by this Declaration of Trust.

6. The power to employ and pay reasonable fees to accountants, lawyers, or investment experts for information or advice relating to the trust.

7. The power to deposit and hold trust funds in both interest-bearing and non-interest-bearing accounts.

8. The power to deposit funds in bank or other accounts uninsured by FDIC coverage.

9. The power to enter into electronic fund transfer or safe deposit arrangements with financial institutions.

10. The power to continue any business of the Grantor.

11. The power to institute or defend legal actions concerning the trust or Grantor's affairs.

12. The power to diversify investments, including authority to decide that the trust property need not produce income.

(C) Payment by Trustee of the Grantor's Debts and Taxes

The Grantor's debts and death taxes shall be paid by the Trustee however the Trustee deems appropriate.

VIII. General Administrative Provisions

(A) Controlling Law

The validity of The XYZ Trust shall be governed by the laws of [STATE].

(B) Severability

If any provision of this Declaration of Trust is ruled unenforceable, the remaining provisions shall nevertheless remain in effect.

(C) Amendments

The term "Declaration of Trust" includes any provisions added by amendments.

(D) Accountings

No accountings or reports shall be required of the Trustee.

Certification by Grantor

I certify that I have read this Declaration of Trust for The XYZ Trust, created January 1, 2019, and that it correctly states the terms and conditions under which the trust property is to be held, managed, and disposed of by the trustee, and I approve the Declaration of Trust.

Dated: January 1, 2019

_____

Grantor – [YOUR NAME]

(New page)

Schedule A

All the Grantor's interest in the following property:

[List the financial accounts or real estate titled to the trust.]

You likely noticed that these two trust documents look very similar. The key differences are minimal, but very important. In the first living trust, you were the trustee. In the second trust, you designated someone else as the trustee. When a trust is used to purchase an asset that requires documentation with the government, such as a house, vehicle, or boat, the trustee's name is usually registered along with the trust. If you plan to use a trust as part of your privacy strategy, you likely do not want to be listed as the trustee. In a later chapter, I will explain the entire process of purchasing a home with a trust. This action will completely hide the owner (you) from any public records associated with the home. We are not ready for that yet, but this familiarization with trusts will aid during that chapter.

Regardless of the route you take to establish a trust, I never recommend obtaining an Employer Identification Number (EIN) from the Internal Revenue Service (IRS). Doing so executes an annual tax reporting requirement, which can complicate your taxes. It also complicates the process of revoking the trust. Since the trust will never be used to generate income, acquire credit, or hire employees, this number is not necessary.

Appointment of a New Trustee

As the grantor of a revocable trust, you have the right to make any changes to it as desired. This includes the ability to change the trustee. There are many reasons one may choose a different trustee. An elderly person may designate a new trustee during the final years of life in order to allow a loved one to sign on behalf of the trust. This could be convenient for making payments when the grantor is unable to complete the process. For our purposes, there is a privacy-related reason that may require you to assign a new trustee.

If you created a trust and assigned yourself as trustee, you may have a situation that warrants the appointment of a new trustee. During the upcoming anonymous house purchase chapter, I explain how a client needed to create a trust and open a checking account in the name of that trust. She made herself the trustee in order to open the bank account, but wanted to assign another trustee before she purchased and deeded a new home in the name of the trust. This would allow her trustee to sign on behalf of the trust on any publicly recorded documents.

The following pages present two amendments to a trust. The first appoints a new trustee, eliminating yourself from the position. The second reverses this decision and places the original trustee (you) back to the position. You may never need these, but know that the option is available.

The XYZ Trust

Amendment to Trust - Appointment of New Trustee

This amendment to The XYZ Trust, dated January 1, 2019, is made this day, [CURRENT DATE], by [YOUR NAME], the grantor of the trust. Under the power of amendment reserved to the grantor by Section III, Paragraph (A), of the trust, the grantor amends the trust as follows:

[YOUR NAME], the grantor and creator of The XYZ Trust, which was created by virtue of a Trust Agreement dated January 1, 2019, and which named [YOUR NAME] as Trustee, hereby terminates the duties of [YOUR NAME] as trustee under said Trust and further hereby appoints [NEW TRUSTEE] as Trustee under the provisions of the Trust Agreement dated January 1, 2019 and known as The XYZ Trust. [YOUR NAME] remains the grantor of The XYZ Trust. In all other respects, the Declaration of Trust as executed on January 1, 2019, by the grantor is affirmed. This amendment was executed on [CURRENT DATE].

_____

[YOUR NAME], Grantor of The XYZ Trust

_____

[WITNESS NAME], Witness

I HEREBY CERTIFY that on this day before me, an officer duly qualified to take acknowledgement, personally appeared the subjects listed above, to me known to be the persons described in, and who executed the foregoing instrument, and acknowledged before me that executed the same. WITNESS my hand and official seal this [CURRENT DATE].

_____

Notary Public

The XYZ Trust

Amendment to Trust - Appointment of New Trustee

This amendment to The XYZ Trust, dated January 1, 2019, is made this day, [CURRENT DATE], by [YOUR NAME], the grantor of the trust. Under the power of amendment reserved to the grantor by Section III, Paragraph (A), of the trust, the grantor amends the trust as follows:

[YOUR NAME], the grantor and creator of The XYZ Trust, which was created by virtue of a Trust Agreement dated January 1, 2019, and which named [PREVIOUS TRUSTEE NAME] as Trustee via amendment on [DATE OF PREVIOUS AMMENDMENT], hereby terminates the duties of [PREVIOUS TRUSTEE] as trustee under said Trust and further hereby re-appoints himself, [YOUR NAME], as Trustee under the provisions of the Trust Agreement dated January 1, 2019 and known as The XYZ Trust. [YOUR NAME] remains the grantor of The XYZ Trust. [ORIGINAL SUCCESSOR TRUSTEE NAME] remains the successor Trustee. In all other respects, the Declaration of Trust as executed January 1, 2019, by the grantor is affirmed. This amendment was executed on [CURRENT DATE].

_____

[YOUR NAME], Grantor and New Trustee of The XYZ Trust

_____

[WITNESS NAME], Witness

I HEREBY CERTIFY that on this day before me, an officer duly qualified to take acknowledgement, personally appeared the subjects listed above, to me known to be the person described in, and who executed the foregoing instrument, and acknowledged before me that executed the same. WITNESS my hand and official seal this [CURRENT DATE].

_____

Notary Public

Certification of Trust

A certification of trust is not a required document in order to possess a valid trust. It is optional, but likely more powerful than the trust itself for our purposes. It is an abbreviated version of the trust document, which contains minimal information about the trust. You may find one useful when transferring property to your trust, such as your home. County and state offices, banks, or other institutions may require proof that the trust exists. The purpose of a certification of trust is to establish that the trust exists, without revealing the personal details, such as the other assets in it and your beneficiaries. Privacy-minded people do not want to reveal this core information to institutions that require proof of the trust's existence, so they submit a certification of trust rather than a copy of the entire trust.

Most states have statutes that set out the requirements for a certification of trust. Some states also provide a specific form in their statutes. If yours does, you should use that form so that your certification looks familiar to the institutions that will see it. If your state does not provide a form, you can make your own using the following guides. In my experience, state-specific forms are not required. Typically, certifications of trust display the following details.

- The name of the trust
- The date the trust was created
- The trustee's name
- The trustee's powers
- The trustee's signature
- A Notary's signature and stamp

Imagine that you are purchasing a home, and the title company demands proof of the trust. Most people just provide a full copy of the entire trust, including the grantor's name (you), your beneficiaries, your successor trustee, and any other private details. This is unnecessary and invasive. The certification of trust includes all information required by various entities without exposing private details. When executing a home purchase for a client, no entity ever sees the full trust document.

CERTIFICATION OF TRUST

STATE OF _____)
) SS.
COUNTY OF _____)

The undersigned, after first being duly sworn and upon their oath, state as follows:

1) THE [NAME OF YOUR TRUST] TRUST was formed on [DATE] and is in existence as of today.

2) THE [NAME OF YOUR TRUST] TRUST is a REVOCABLE Trust.

3) The sole Trustee, [NAME OF YOUR TRUSTEE], has full authority and power to convey real estate owned by this trust, the power to acquire additional property, the power to sell and execute deeds, the power to execute any documents, and the power to deposit and hold trust funds.

4) Title to Trust assets is to be taken as follows: THE [NAME OF YOUR TRUST] TRUST.

5) The Trust has not been revoked, modified or amended in any manner which would cause the representations contained herein to be incorrect.

6) I am the only currently acting trustee.

Dated: [DATE]

_____

[NAME], Trustee of THE [NAME OF YOUR TRUST] TRUST

_____

Notary Public

Let's dissect this document.

- The first section identifies the state and county where the trust was established. This also identifies the state trust laws that would apply to the trust. This is usually the location of the trustee, but can also be the county of the grantor (you).
- Number 1 identifies the name and date of the trust. These two pieces are vital and should be the same on all documents.
- Number 2 declares that the trust is revocable, and that it can be modified at any time by the grantor.
- Number 3 identifies the current trustee and states his or her power. This is vital to establish to the requesting institution that the trustee has the authority to sign on behalf of the trust.
- Number 4 defines the name of the trust as it should appear on any titles or deeds.
- Number 5 confirms that the trust is valid as of the date signed. Some entities will require a version of this certification that has been recently signed.
- Number 6 confirms that there are not additional trustees. If there were, they would also need to be listed and approve any transactions or purchases.
- The date should be the date signed, and does not need to match the previous date of when the trust was established.
- This form should be notarized, as many institutions will not accept it if it is not.

The name of the trustee will vary depending on the way your trust was defined. If you made yourself the trustee, then you would sign this document. If you assigned a trustee other than yourself for privacy purposes, that person must sign the document. Both of these scenarios will be discussed in the vehicle and home purchase chapters.

This is a great time to remind readers that this entire book should be read, digested, and understood before attempting any of this on your own. Please remember that these are simply examples of documents and scenarios associated with my clients. It is very possible that these examples will not be appropriate for your personal needs. A competent estate attorney should confirm the most appropriate path for you.

Choosing a Trustee

You have now learned of the various ways that trusts can be created and later chapters will demonstrate their power during asset purchase and ownership. An important consideration I have glossed over until now is choosing a trustee for your trust. This is a decision that should not be made in haste. You should place much thought into this, as the trustee will need to be involved with any asset purchases.

Before you stress about this too much, know that as the grantor of a revocable trust, you can replace the trustee at any time. You still have the power to make any changes desired. Your choice of trustee might vary based on the purpose of the trust. Consider the following scenarios.

- You are establishing a trust to purchase a home. You do not want your name publicly associated with the purchase or the deed. The home will be titled into the trust name. The county of this home demands to include the trustee's name on the deed, similar to "The #65436 Trust, Jane Doe, Trustee". The trustee will need to sign several documents at closing, which will all be publicly recorded at the county level. You plan to place the utilities within the name of the trust, and the certification of trust will be used as proof of existence. Obviously, you will need a trustee that is available to you and willing to assist.
- You are purchasing a vehicle and plan to title it into the trust. You do not want your name publicly associated with the vehicle's title or registration with the state. The state requires a trustee's name on the application, but does not publish the name of the trustee on the title or registration. The trustee will need to sign the application and provide valid government identification during the process.

While both of these require a cooperative and willing trustee, the second will document an SSN or driver's license number of the trustee. This places more responsibility on the trustee, and possibly some discomfort. The first scenario will not require anything more than a Notary approval of the trustee's signature, and provides some distance between the true identity of the trustee and the purchase. In all scenarios, you must choose an appropriate trustee.

Your trustee will play a vital role in carrying out the execution of a purchase titled in your trust. In most situations, the trustee does not need experience in financial management or private purchases. That is YOUR job. However, they do need to possess common sense, dependability, and trust in your actions. You will be asking your trustee to sign documents that he or she may not fully understand. While you should fully trust your trustee to carry out your instructions, the relationship must be respectful both ways. You would never want your trustee unsure of your plan or execution. Choosing your trustee can be one of the most

difficult decisions throughout this process. I cannot offer a black-and-white playbook for this, but I can offer some suggestions.

Family: This is a bit dangerous in terms of privacy, but usually the easiest. If you have a close relative that is willing to be your trustee in order to disguise your name from public records, this can work. Before you commit, identify any potential exposure online. Search your name and the family member's name within every people search site and see if there is a connection between the two of you. If so, it is not necessarily a deal-breaker, but something important to consider. Will your adversary identify your family, search for trusts in their name, and assume that you live at the house? Most will not go that far, but some have. If you are running from the paparazzi or a private investigator, they will absolutely follow these paths. If you choose a family member, one with a different last name is always preferred. Since I have a unique last name, and new people search sites with family connections pop up every day, this route was not for me.

Friend: This path can offer a bit more privacy, especially if there are no online associations. If photos of you and your friend are all over Facebook, this is not a wise choice. If you choose to make a friend your trustee, this should be a strong friendship that has a long history. I have people in my life that would proudly serve this role, but the weak link will always bother me. Anyone that had the time to research my past, and search for these names on public records associated with trusts outside of the general areas of the potential trustee, could possibly identify my trust and home. This is a bit far-fetched, but on my mind. If my friend's name was John Wilson, that may sway my thinking. If you have a trusted friend with that common of a name, congratulations. You may have found your trustee.

Attorney: This is a more expensive option, but provides stronger privacy. My trustee is an attorney who specializes in estate planning. For a fee, he agreed to scrutinize my documents and act as a trustee on my behalf. He signed my closing documents on my home as the trustee of my trust, and his name is on record with the county (but no trustee name is listed on the deed). We possess a private contract eliminating any liability on his behalf. He also has possession of my full trust(s) which outline my wishes upon death. The attorney-client privilege offers yet another layer of trust between us. Most estate planning attorneys do not offer this level of service, so you will spend some time hunting for this. When you find it, you have achieved a great layer of protection between you and your home.

Your trustee should be whoever you feel is most trustworthy to do the job, is willing to do it, and will respect your privacy once the job is finished. If using a trust to buy a home, your trustee will likely know the address. This person is now the weakest link. A social engineering attack on him or her could reveal something you have spent countless hours trying to hide. Please choose wisely.

Limited Liability Companies (LLCs) - New Mexico

Privacy enthusiasts have heard for years that a New Mexico LLC is a powerful tool to help hide the true owner of your home. This can be accurate, but it is not the only option. Furthermore, New Mexico is not the only state that offers fairly anonymous LLCs. For many of my clients, an LLC was not the most appropriate fit. I have owned numerous LLCs and used them to title homes, vehicles, and utilities for myself and clients. This section will first explain the power of an "invisible" LLC, then the practical usage, and finally the details of establishing this entity.

Every state has the ability to create an LLC. Each state has their own requirements, and this can vary from full disclosure of all members to no owner disclosure whatsoever. This is the first step toward choosing the appropriate state for your LLC. Overall, we only want to consider states that do not require public disclosure of the owners or members. States such as California and Illinois demand that you publicly disclose the full name and physical address of each member of the LLC. This provides no privacy protection and anyone can search your name to find your LLC in seconds. States such as Delaware, Nevada, New Mexico, and Wyoming do not require you to disclose any details of the members of the LLC. They each only require you to possess a registered agent within the state of your filing. This is easy and fairly affordable.

Since we have limited our choice to four states, the next consideration is cost. Delaware requires a yearly $300 fee, regardless whether you use the LLC in any way. Nevada is more expensive and Wyoming is much more affordable, but you will need to find a "nominee" to replace you on the public forms with both. This can be completed fairly anonymously, but I have a better option. New Mexico has the most lenient requirements and has no annual filing fee. For most clients that need an LLC, New Mexico is the best choice.

First, you must find a company that provides New Mexico LLC creation services. There are many, and I will not name any specific providers. I will only say that each of them provides an almost identical service. However, the fees for the services are not identical. I have seen companies demand $300-$800 to initiate the LLC and then an annual fee of over $400. This is the high side of this service. The more affordable options cost between $150 to $200 to form the LLC with an annual fee of $30 to $50 for the registered agent service. An online search of "New Mexico Private LLC" will present many options. Do your homework, check reviews, and find the best option for your needs.

A reputable LLC provider will do all of the hard work for you. You will pay the initial fee and they will automatically serve as your New Mexico registered agent and your LLC organizer. That means that the only identifying information listed on your Articles of Organization provided to the state is their information. Your information remains private from the state.

The provider will obtain the LLC from the New Mexico Corporations Bureau in the name you requested. This is the first choice you need to make.

The name of your LLC is important. It should be vague and not have any personal association to you. If you plan to use this LLC as part of your purchase of an anonymous home, you may want to tailor the name toward that strategy. Names such as "Southwest Real Estate Ventures LLC" or "Wilson Home Builders" could be appropriate for utilities and home services. Names such as these appear legitimate versus a suspicious choice such as "Extreme Privacy Seekers LLC". The following website will allow you to search for a name to make sure it is not already in use:

https://portal.sos.state.nm.us/BFS/online/CorporationBusinessSearch

Once you have chosen your LLC name and paid the fee to the registered agent, you will need to provide your contact information before they will file for the LLC. The service will want your full name, physical address, email address, and telephone number. Reputable privacy-oriented LLC creation companies will not share these details with the state or any third parties, but check any privacy policies to know what will be done with your data. You should choose this contact information carefully.

There is debate about whether you must be honest with these details. You are providing contact information to a private company that does not share it with the state. You could probably get away with an alias. However, I do not recommend this. The reason they need this information is to meet the requirements from New Mexico. The service must know the identity of the creator of the LLC in order to serve any legal process that could arrive. While that is likely outside the scope of your scenario, it is possible that someone could file a lawsuit against your LLC. If so, a subpoena could be issued to your registered agent on your behalf. That agent would then forward the legal paperwork to you. I have created LLCs using both real and alias information, but I now recommend using your true identity (to an extent).

- For the name, I would provide your first initial and last name. Your physical address can be a PO Box or CMRA. If you only have a PMB as discussed previously, you could use that. However, I prefer to only use a PMB for things that are heavily associated with your true name. If you have a local PO Box that you use to receive your mail from the PMB, that is a much better option. Your email address can be a ProtonMail account created just for this purpose, and your telephone number can be a MySudo or other VOIP number. Payment can be made using a prepaid gift card or a Privacy.com account (discussed later).

None of these details will be filed with the state, and none will be visible within public records. Only your registered agent will have these details, which is another reason to spend time picking the right service for your needs. I also recommend calling any potential registered

agents and asking them about their ability to keep your details private. If you are unable to reach a human and cannot receive an acceptable answer, keep looking. You will know when you find the right fit.

The registered agent service will file your LLC with the state, including the "Articles of Organization", and provide you copies of this document and the "Certificate of Organization". Most reputable LLC creation companies will provide the documents needed, but some may ask you to complete the Articles of Organization, which can be found at the following website.

http://www.sos.state.nm.us/uploads/files/Corporations/dllc.pdf

Vague examples of the Articles or Organization (which are submitted to the state) and the Certificate or Organization (which is received from the state) are included within the following pages. Your versions may vary slightly. Note that the content on the following pages contains all of the mandatory disclosures. Any other details, such as the names of the members, are optional and should not be included.

As a reminder. the following pages only apply to LLCs created in New Mexico. Researching other states should provide similar documents in order to understand the key differences from one state to another. Additionally, these examples are only to be used as tools for privacy, and never to generate any income. I will discuss more on that scenario in a later chapter. If you have chosen the South Dakota nomad route, creating your LLC in that state has many benefits. In the next chapter, I explain each step of using a South Dakota LLC to register your vehicle without ever disclosing your name.

Finally, please do not use these examples as legal advice or absolute verbiage for your own documents. State laws, forms, and regulations change often. I share these only as a learning tool.

The New Mexico Secretary of State website contains a wealth of information online at http://www.sos.state.nm.us/Business_Services/NM_Domestic_LLC.aspx. I encourage you to read through each document before considering your own LLC strategy.

ARTICLES OF ORGANIZATION

SOUTHWEST REAL ESTATE VENTURES LLC

The undersigned, acting as organizer of a limited liability company pursuant to the New Mexico Limited Liability Act, adopts the following Articles of Organization:

The name of the Limited Liability Company is:

SOUTHWEST REAL ESTATE VENTURES LLC

The latest date upon which the company is to dissolve is December 31, 2120.

The name of the registered agent for the LLC is:

[YOUR REGISTERED AGENT BUSINESS NAME]

The New Mexico street address of the company's initial registered agent is

[ADDRESS OF YOUR AGENT]

The street address of the company's principal place of business is

[ADDRESS OF YOUR AGENT]

The mailing address of the Limited Liability Company is

[ADDRESS OF YOUR AGENT]

The LLC will be managed by Member(s).

OFFICE OF THE PUBLIC REGULATION COMMISSION

CERTIFICATE OF ORGANIZATION

OF

SOUTHWEST REAL ESTATE VENTURES LLC

#876345

The Public Regulation Commission certifies that the Articles of Organization, duly signed & verified pursuant to the provisions of the

LIMITED LIABILITY ACT
(53-19-1 TO 53-19-74 NMSA 1978)

Have been received by it and are found to conform to law.

Accordingly, by virtue of the authority vested in it by law, the Public Regulation Commission issues this Certificate of Organization and attaches hereto, a duplicate of the Articles of Organization.

Dated: April 1, 2019

In testimony whereof, the Public Regulation of the state of New Mexico has caused this certificate to be signed by its Chairman and the seal of said Commission to affixed at the City of Santa Fe.

_____
Chairman

_____
Bureau Chief

The Certificate of Organization includes the state issued number to your LLC. This document will be used when an entity, such as the DMV, insists on something official in relation to your LLC. This document can be verified online and duplicates with a more recent date can be ordered. Notice that no personal information appears on these documents.

Technically, you now have an official LLC through the state of New Mexico. You will need to pay the minimal fee to your registered agent every year in order to be legal, and you will likely never need the agent's services again. Now that you own the LLC, you should consider the next steps.

While your registered agent and the state of New Mexico did not require you to disclose an Operating Agreement for your LLC, you should create one right away. This document outlines the terms of the LLC, owner information, and rules of how the LLC will be maintained. Theoretically, no one should ever need to see this document, but having it could assist you in the rare case that any legal battles come your way. I have used a very simple template for all of my LLCs, and I have never needed to display a copy to anyone. If you choose to open a bank account under this LLC, they may want to see this document. I will discuss more on that in a later chapter.

Overall, the operating agreement contains details which identify you as the owner, and can serve as proof of ownership if the need should arise. Much of it is legal speak in order to satisfy requirements of financial institutions. I prefer to create and notarize this document before the Certificate of Organization is issued. Within the document, I present a brief summary of each item, and why it is important, within brackets.

The following example is for a single-member LLC. It is the easiest way to establish an LLC for privacy purposes. You should contact an attorney before executing your own operating agreement in order to ensure that it is appropriate for your unique situation. Creating a complete LLC package, including optional documents which may never be seen by anyone except you, is important. If anyone should challenge your ownership of an asset, through the invisible LLC which has control of it, you want proper legal documents in your possession. Possessing these documents, which are notarized during the creation of the LLC, and not created only as a response to some negative attention, will weigh heavily in your favor. Double-check all dates to make sure there are no conflicts which could raise scrutiny if challenged. Again, this is where an experienced attorney can be beneficial. My first several attempts at LLC creation in 2008 are laughable now and could be deemed illegal, likely having no power in a courtroom.

LIMITED LIABILITY COMPANY OPERATING AGREEMENT

FOR

SOUTHWEST REAL ESTATE VENTURES LLC

A Member-Managed Limited Liability Company

ARTICLE I: Company Formation

1.1 **FORMATION**. The Members hereby form a Limited Liability Company ("Company") subject to the provisions of the Limited Liability Company Act as currently in effect as of this date. Articles of Organization shall be filed with the Secretary of State.

[This establishes the formation.]

1.2 **NAME**. The name of the Company shall be:

SOUTHWEST REAL ESTATE VENTURES LLC

[This establishes the name.]

1.3 **REGISTERED AGENT**. The name and location of the registered agent of the Company shall be:

[NAME OF YOUR AGENT]
[ADDRESS]

[This establishes the registered agent.]

1.4 **TERM**. The Company shall continue for a perpetual period.

[This establishes the LLC does not have a pre-determined termination date.]

1.5 **BUSINESS PURPOSE**. The purpose of the Company is hold assets.

[This establishes the purpose of the business and declares it is not designed to generate income.]

1.6 **PRINCIPAL PLACE OF BUSINESS**. The location of the principal place of business of the Company shall be:

[YOUR PO BOX]

[This establishes an address for the LLC (not the registered agent address). This can be a PO Box.]

1.7 **THE MEMBERS**. The name and place of residence of each member are contained in Exhibit 2 attached to this Agreement.

[This references an additional exhibit attached to this agreement, explained later.]

1.8 **ADMISSION OF ADDITIONAL MEMBERS**. Except as otherwise expressly provided in the Agreement, no additional members may be admitted to the Company through issuance by the company of a new interest in the Company, without the prior unanimous written consent of the Members.

[This prevents adding additional members without your consent.]

ARTICLE II: Capital Contributions

2.1 **INITIAL CONTRIBUTIONS**. The Members initially shall contribute to the Company capital as described in Exhibit 3 attached to this Agreement.

[This references an additional exhibit attached to this agreement, explained later.]

2.2 **ADDITIONAL CONTRIBUTIONS**. Except as provided in ARTICLE 6.2, no Member shall be obligated to make any additional contribution to the Company's capital.

[This prevents a requirement for you to contribute additional funding to the LLC.]

ARTICLE III: Profits, Losses and Distributions

3.1 **PROFITS/LOSSES**. For financial accounting and tax purposes the Company's net profits or net losses shall be determined on an annual basis and shall be allocated to the Members in proportion to each Member's relative capital interest in the Company as set forth in Exhibit 2 as amended from time to time in accordance with Treasury Regulation 1.704-1.

[This should not be required, but defines how profits and losses will be allocated if the LLC ever generates income or losses.]

3.2 **DISTRIBUTIONS**. The Members shall determine and distribute available funds annually or at more frequent intervals as they see fit. Available funds, as referred to herein, shall mean the net cash of the Company available after appropriate provision for expenses and liabilities, as determined by the Managers.

[This should not be required, but defines how funds will be distributed if the LLC ever generates income or losses.]

ARTICLE IV: Management

4.1 **MANAGEMENT OF THE BUSINESS**. The name and place of residence of each Manager is attached as Exhibit 1 of this Agreement. By a vote of the Members holding a majority of the capital interests in the Company, as set forth in Exhibit 2 as amended from time to time, shall elect so many Managers as the Members determine, but no fewer than one, with one Manager elected by the Members as Chief Executive Manager. The elected Manager(s) may either be a Member or Non-Member.

[This allows you to be elected as Chief Executive Manager.]

4.2 **POWERS OF MANAGERS**. The Managers are authorized on the Company's behalf to make all decisions as to (a) the sale, development lease or other disposition of the Company's assets; (b) the purchase or other acquisition of other assets of all kinds; (c) the management of all or any part of the Company's assets; (d) the borrowing of money and the granting of security interests in the Company's assets; (e) the prepayment, refinancing or extension of any loan affecting the Company's assets; (f) the compromise or release of any of the Company's claims or debts; and, (g) the employment of persons, firms or corporations for the operation and management of the company's business. In the exercise of their management powers, the Managers are authorized to execute and deliver (a) all contracts, conveyances, assignments leases, sub-leases, franchise agreements, licensing agreements, management contracts and maintenance contracts covering or affecting the Company's assets; (b) all checks, drafts and other orders for the payment of the Company's funds; (c) all promissory notes, loans, security agreements and other similar documents; and, (d) all other instruments of any other kind relating to the Company's affairs, whether like or unlike the foregoing.

[This section defines the powers of Managers.]

4.3 **CHIEF EXECUTIVE MANAGER**. The Chief Executive Manager shall have primary responsibility for managing the operations of the Company and for effectuating the decisions of the Managers.

[This section defines the responsibility of the Chief Executive Manager.]

4.4 **INDEMNIFICATION**. The Company shall indemnify any person who was or is a party defendant or is threatened to be made a party defendant, pending or completed action, suit or proceeding, whether civil, criminal, administrative, or investigative (other than an action by or in the right of the Company) by reason of the fact that he is or was a Member of the Company, Manager, employee or agent of the Company, or is or was at the request of the Company, for instant expenses (including attorney's fees), judgments, fines, and amounts paid in settlement actually and reasonably incurred in connection with such action, suit or proceeding if the Members determine that he acted in good faith and in a manner he reasonably believed to be in or not opposed to the best interest of the Company, and with respect to any criminal action proceeding, has no reasonable cause to believe his/her conduct was unlawful. The termination of any, suit, or proceeding by judgment, order, settlement, conviction, or upon a plea of "no lo Contendere" or its equivalent, shall not in itself create a presumption that the person did or did not act in good faith and in a manner which he reasonably believed to be in the best interest of the Company, and, with respect to any criminal action or proceeding, had reasonable cause to believe that his/her conduct was lawful.

[An indemnification provision, also known as a hold harmless provision, is a clause used in contracts to shift potential costs from one party to the other. This example states that the LLC will not seek damages from you. This is largely unnecessary for our purposes, but standard verbiage.]

4.5 **RECORDS**. The Managers shall cause the Company to keep at its principal place of business the following:

(a) a current list in alphabetical order of the full name and the last known street address of each Member;

(b) a copy of the Certificate of Formation and the Company Operating Agreement and all amendments;

(c) copies of the Company's federal, state and local income tax returns and reports, if any, for the three most recent years;

(d) copies of any financial statements of the limited liability company for the three most recent years.

[This states that you will maintain proper records.]

ARTICLE V: Bookkeeping

5.1 **BOOKS**. The Managers shall maintain complete and accurate books of account of the Company's affairs at the Company's principal place of business. Such books shall be kept on such method of accounting as the Managers shall select. The company's accounting period shall be the calendar year.

[This also defines that you will keep proper books and that your business year will follow a traditional calendar year. This is important for businesses that make a profit, but likely not needed in an LLC made for privacy.]

CERTIFICATE OF FORMATION

This Company Operating Agreement is entered into and shall become effective as of the Effective Date by and among the Company and the persons executing this Agreement as Members. It is the Members express intention to create a limited liability company in accordance with applicable law, as currently written or subsequently amended or redrafted.

The undersigned hereby agree, acknowledge, and certify that the foregoing operating agreement is adopted and approved by each member, the agreement consisting of ___ pages, constitutes, together with Exhibit 1, Exhibit 2 and Exhibit 3 (if any), the Operating Agreement of SOUTHWEST REAL ESTATE VENTURES LLC, adopted by the members as of April 1, 2019.

Members:

_____ _____

[YOUR NAME] **Date**
Percent: 100%

[This is the official signature page that executes this document. It should be notarized.]

_____ _____

Notary Public **Date**

EXHIBIT 1

LIMITED LIABILITY COMPANY OPERATING AGREEMENT

FOR

SOUTHWEST REAL ESTATE VENTURES LLC

LISTING OF MANAGERS

By a majority vote of the Members the following Managers were elected to operate the Company pursuant to ARTICLE 4 of the Agreement:

_____

[YOUR NAME]

Chief Executive Manager

[YOUR PO BOX ADDRESS]

[This defines you as the Chief Executive Manager.]

Notary Public **Date**

EXHIBIT 2

LIMITED LIABILITY COMPANY OPERATING AGREEMENT

FOR

SOUTHWEST REAL ESTATE VENTURES LLC

LISTING OF MEMBERS

As of the 1st day of April, 2019 the following is a list of Members of the Company:

[YOUR NAME] **Percent** 100%

[YOUR PO BOX ADDRESS]

_____

Signature of Member

[This defines you as the sole member of the LLC. It should be notarized.]

_____ _____

Notary Public **Date**

EXHIBIT 3

LIMITED LIABILITY COMPANY OPERATING AGREEMENT

FOR

SOUTHWEST REAL ESTATE VENTURES LLC

CAPITAL CONTRIBUTIONS

Pursuant to ARTICLE 2, the Members' initial contribution to the Company capital is stated to be $_____.00. The description and each individual portion of this initial contribution is as follows:

[YOUR NAME] _____ $ .00

SIGNED AND AGREED this 1st day of April, 2019.

_____

[YOUR NAME]

[This defines the initial funding of the LLC, if applicable, such as an initial deposit into a checking account in the name of the business.]

_____ _____

Notary Public **Date**

Let's take a breath and look at what we have accomplished. You chose a name for your LLC and hired a Registered Agent service to file the paperwork on your behalf. They know your true identity, but no personal details were disclosed to the state of New Mexico. You created an operating agreement that outlines the legal details of your LLC. This is a personal document which is never shared with the state or the registered agent. You may never need to show this to anyone. You now have an official LLC that is ready to be used. The next consideration is an Employer Identification Number (EIN) with the Internal Revenue Service (IRS). This is a delicate decision that should not be made without serious thoughts.

Your LLC does not require an EIN if you do not plan for it to generate any income. For the purposes of this chapter, you should never be paid by any entity in the name of this LLC. You can place assets in the LLC without an EIN. If you do not possess an EIN, there is no mandatory reporting or tax filing with the IRS. Obviously, if you obtain an EIN, the IRS will know that you are directly associated with the LLC. They will demand your SSN and other details as part of the application. As you can see, there are many benefits to NOT obtaining an EIN for your new LLC.

There are also some advantages. An EIN can go a long way when you want to provide legitimacy for the LLC. If you plan to open utilities in the name of an LLC, the first question from the utility company will be, "What is your EIN?". Without an EIN, they will start demanding your SSN. If you have any plans of opening a bank account in the name of the LLC, the bank will also require an EIN.

Another benefit of an EIN is to provide proof of ownership. If you plan to place a $1 Million home in the name of an LLC, and someone challenges you and claims THEY are the owner, you have a great resource (IRS) that can verify the EIN of the true owner. If you decide to obtain an EIN, make sure to notify your tax preparer. While you will not owe any federal taxes on an LLC that does not generate income, the IRS will expect to see a claim of this on your yearly tax filing. In this situation, your LLC is a pass-through entity to you as the sole member.

The procedure to obtain an EIN from the IRS is very simple, and the result is immediate. The following website has all of the details.

https://www.irs.gov/businesses/small-businesses-self-employed/apply-for-an-employer-identification-number-ein-online

Overall, I do NOT recommend obtaining an EIN unless you know you will need it. You can apply for this number at any time, regardless of when the LLC was created. If you plan to title a vehicle in an LLC, connect a bank account to the LLC, or register utilities in the name of the LLC, an EIN will probably be required.

Limited Liability Companies (LLCs) - South Dakota - Nomads

The previous pages applied specifically to New Mexico. There are many privacy benefits with that state and you do not need to renew your LLC every year. It is a great choice for those who live in practically any state. However, nomads of South Dakota may choose their own state for LLC creation. The process is much simpler and you can still possess privacy. Much of the process is similar to the previous option, but you may notice many fewer steps and demands. The entire process can be completed online, and you will receive your LLC documents immediately. Begin at the following website.

https://sosenterprise.sd.gov/BusinessServices/Business/RegistrationInstr.aspx

- Choose the "Start a new business" button.
- Choose "Domestic LLC" and click "Next".
- Enter your desired LLC name after you have used the search tool to verify availability.
- Leave "Professional Type" as "none" and click "Next".
- Provide your PMB address or a new PMB address reserved for your LLC.
- Provide your registered Agent's name. Most PMB's offer this service. Select the "Non-Commercial" option and enter the name of your agent provided by your PMB. Conduct a search and choose the appropriate option.
- Choose your Organizer's name. You can select an individual or a company for this. South Dakota allows you to specify your own LLC as the organizer, which I find interesting. If you would rather assign an individual, you can add your own name or another "nominee". I have a close friend with a very generic name such as John Wilson. I pay him a small annual fee to be my "Contract Officer", and he has the authority to "Organize" my business. His address is not required.
- Choose "Perpetual" in order to set no specific expiration date.
- Select the "Member-Managed" option and "No".
- Ignore the "Beneficial Owners" option.
- Ignore the "Additional Articles" option.
- Ignore the "Recipient" option.
- Confirm all of your details and click "Next".
- Provide a digital signature. This is a digital input and no "wet" signature is required. The name you provide will be publicly recorded. I ask my Contract Officer to be the authorized signee on my LLCs and he allows me to digitally sign on his behalf.
- Make your payment with a credit card, prepaid card, or Privacy.com card, depending on your desired level of privacy.

After successful payment, you will immediately receive a digital copy of your Articles of Organization and Certificate of Organization. You now possess an official and legal LLC in the state of South Dakota. This is the quickest way to obtain an LLC, and is yet another benefit of South Dakota nomad registration. This may all seem too good to be true. Well, there are a few privacy considerations.

- With the New Mexico option, you hired a middle-man to serve as your agent. The process took weeks to complete. He or she demanded to know your true identity, but withheld it from the state. In this scenario, the agent at your PMB plays this role. He or she will also demand to know your true identity. The fee for this service is usually quite minimal, and much more affordable than any New Mexico options. Be sure to enable the registered agent service with your PMB provider before executing the LLC.
- Your PMB address will be publicly visible. This may identify you as the owner if your PMB is also associated with your name in public records. Many of my clients open a second PMB address solely for LLC use. You will still need to disclose your real name to the PMB provider and complete the USPS form 1583 as we did previously. However, this prevents anyone from publicly associating the personal PMB with the LLC PMB. In my experience, contacting your PMB provider and stating that you would like to open a second PMB for your LLC can result in a discounted rate.
- South Dakota only requires that your "Organizer" be displayed within public records. There is no identity verification for this person. Play by the rules, but consider a nominee with a common name.
- You should still form your own Operating Agreement as outlined previously. These are applicable to any state.

Renewals

A South Dakota LLC requires annual renewal. The process is conducted completely online. You will be asked if any details of your LLC have changed. If they have not, you simply pay the $50 annual fee and receive updated digital paperwork. You will be asked to provide a name for the renewal report. I have found that either your original organizer or registered agent's name works fine here. The renewal does not require a signature or verification of identity.

I have executed dozens of South Dakota LLCs and I have never run into any issues. The entire process is automated with very little human interaction. However, this does not authorize you to provide false information or to bend any of the rules. The last thing you want is for the state to terminate your LLC due to inaccuracies or fraud. This is especially true if you use this LLC for assets, which is explained later. LLCs are a great vehicle to mask your name from public records, but they always possess a paper trail back to you (as they should). Unless the government issues court orders to your PMB provider and registered agent, your name should never be publicly associated with the LLC, as long as you used a nominee during creation.

Summary

This is an overwhelming chapter. It is very technical, but hopefully provides some insight into the basic foundations of trusts and LLCs. In the next chapter, we can make our first purchase in the name of a trust or LLC, and start to take advantage of these avenues for privacy protection. This should help explain the power of these legal entities. You will likely find that most of the efforts creating LLC operating agreements and trust documents will go unnoticed. In ideal scenarios, no one will ever see your hard work. You will never expose these documents. However, skipping these important steps would be a mistake. If anything should ever backfire, your attention to detail will be in your favor. If you die, leaving these documents for your beneficiaries will be helpful. Understanding these "behind the scenes" documents is vital in order to execute the strategies in future chapters.

You may have noticed I do not offer digital downloads of these templates. This is very deliberate. I encourage people to completely understand the documents they create. Signing a digital template is easier, but more reckless. I encourage people to always create their own documents and only include details they understand completely. Since these examples are not provided as templates for personal use, digital copies are not available. The examples are provided only as a demonstration of my prior usage, and not absolute guidance for your own strategies.

International Considerations: LLCs and trusts are very common in America. However, you may reside in a country which does not acknowledge these specific terms. Most countries possess laws which define legal infrastructures such as sole proprietorships (or sole traders), various types of partnerships, and numerous levels of "limited" companies or organizations. Trusts are widely used internationally, but the documents must conform to the laws created for the specific style of trust. I encourage you to research all options available within your country of residence. Once you find a suitable infrastructure, locate any online templates which should help you understand your own legal document options.

Chapter Six

Private Vehicles

Your current vehicle, which is likely registered in your name and current address, can never be made private. You could request a new title under the name of your trust, but the history can never be erased. The Vehicle Identification Number (VIN) is already within dozens of publicly available databases, many including your name and address. I can search your name to identify the vehicle, search the VIN to identify the new owner (the trust), and associate you with the vehicle forever. This does not mean there are no reasons to re-title a vehicle.

If you own a vehicle that you plan on keeping for several years, I do recommend changing the title from your name to the name of a trust which you have established for the sole purpose of titling the vehicle. This does not prevent someone from identifying you through the vehicle, but it does stop daily invasive behavior. If your license plate is registered to your real name and home address, these details are very exposed. The information behind every license plate can be collected in many ways. Consider the following examples.

- You have a nosy neighbor who runs the local HOA and he is bothered by your desire for privacy and overall seclusion. He wants to know more about you. He asks his cousin, who happens to be a police officer, to search the license plate.
- You live in an urban area surrounded by license plate readers. Cameras posted on street corners or attached to city vehicles capture every plate and amend their database with the date, time, location, and details of the registration (your name and address). This database can be searched by any other entity connected to this national system. A search of your name reveals your travels and history.
- A road rage incident leads to an aggressor capturing your plate and desiring revenge. A $10 online query reveals your full home address details, and possibly an unwanted visit by an unstable person.

Re-titling your vehicle to the name of your trust or LLC will provide a layer of privacy in these types of incidents. You are not bullet-proof thanks to vehicle history databases, but you are better protected from the daily mass attacks against your privacy. It is not as powerful as a new private vehicle purchase, which I will explain within this chapter. I present several scenarios which vary in protection from the least to most private.

Current Vehicle Re-Titling to a Trust

First, let's consider a scenario where you are NOT a nomad as defined previously. You possess a vehicle, without a lien, registered in your real name in the state which you physically reside. This chapter will only focus on vehicles without liens. While you can re-title a vehicle with a lien, you are at the mercy of the bank holding the loan. Many financial institutions refuse this, because it is a small asset compared to something larger such as a house. If you push the issue enough, they will likely allow the transfer, but they will often insist that your name appears on the title as the trustee of the trust. This eliminates the privacy benefits of this technique. Therefore, I will assume that you will be re-titling vehicles that are paid in full.

This first scenario will be short, as each state is unique. Your state's policies can vary greatly from other states. You will need to contact your local DMV to determine the requirements to re-title your vehicle. The steps outlined in the next sections explain a typical process, but every state has their own nuances. Below are the basic considerations which may sway you away from re-titling your current vehicle, and waiting for the next purchase to execute a vehicle into a trust.

- Any state will allow you to transfer the title from your name into your trust.
- Some states will demand that the trustee name be present on the title.
- Some states will see this as a taxable event, and you must convince them otherwise.

If your state demands a trustee present on the title, it may be vital to adopt a trust with someone besides yourself as the trustee, as discussed previously. If your state does not require the trustee name, it may be acceptable to use a trust with you as the trustee since your vehicle is already associated with your true name. The general idea here is that you will go to your local DMV and identify your options. You should request to transfer the title of your current vehicle into your trust. Present your certificate of trust and identification, and begin the process. Ensure they know you will remain the owner and that the vehicle was not "sold" to the trust. My experiences with title transfer in various states has been hit and miss. In some scenarios, the hassle was not worth the reward. Often, I had to educate the employee about trusts, and occasionally I left without a successful transfer. If there is any chance you will be selling the car in the near future, transfer is not always justified. Consider the following tutorials before you contact your state's offices.

Unlike a traditional driver's license, most states allow you to use a verified PO Box as the address on the vehicle title and registration. This is another strong layer of privacy, as your home address is no longer publicly exposed.

Current Vehicle Re-Titling to a Trust (Nomad)

Next, consider a scenario where you plan to become a legal nomad resident of South Dakota. This would also apply to Texas, but the documentation here is specific to South Dakota. Another advantage of South Dakota is the ability to title a vehicle before obtaining official nomad residency. This allows you test the waters a bit before diving in completely. The final vehicle registration can also be used to justify your connection to the state, which can make the driver's license acquisition easier.

After the PMB is in place and tested, I prefer to immediately transfer any vehicles to the new state of future or current domicile. If you are not a resident of South Dakota yet, but possess a valid physical address within the state (PMB), you can register your vehicles right away. First, gather your title and bill of sale from the dealership or individual for your vehicle. The title will be surrendered to the state and the bill of sale will hopefully waive any taxes owed.

Vehicle registration is an important step toward the transition to a new state, as well as a great verification tool that may be needed to show association as a resident. The order of events while establishing residency is crucial. If becoming a nomad in South Dakota, I recommend registering your vehicles BEFORE claiming residency. If you will be seeking nomad status in Texas, you must register your vehicles at the time of claiming residency at the DMV.

You will need the following four forms from the South Dakota Department of Revenue, all of which can be found online on their website at the following address.

https://dor.sd.gov/Motor_Vehicles/Forms/Motor_Vehicle_Forms.aspx

- Affidavit Claiming Lack of Residence Post Office Address (no longer)
- Application for Motor Vehicle Title & Registration
- Applicant's Tax Payment Verification
- South Dakota Exemptions

The nomad affidavit is likely the most foreign document to most clients, and I have included a verbatim copy on the following page. This may require some explanation, which follows. This document is only required if you have not established domicile in the state.

AFFIDAVIT CLAIMING LACK OF RESIDENCE POST OFFICE ADDRESS

I, _____, in conjunction with my South Dakota Application for Title and Registration, do hereby declare and affirm that the following facts are true:

1. I do not have a South Dakota Driver's License; and

2. I do not maintain a "residence post office address" in South Dakota or any other United States jurisdiction; and

3. Because I do not maintain a "residence post office address" in South Dakota or any other United States jurisdiction, the address I have provided with my South Dakota Application for
Title and Registration is strictly for mail-forwarding purposes.

_____
Signature of Affiant

_____
Date

_____
Printed Name of Affiant

_____
Notary Public or County Treasurer

STATE OF SOUTH DAKOTA; COUNTY OF _____ Subscribed and Sworn to before me this __ day of _____, 20__.

_____
Date Commission Expires

This document is basically a statement of intent. It has three requirements, which I will explain individually. The first is fairly obvious, as you do not possess a South Dakota license (yet). If you already have one, this document is unnecessary. The second requirement is where we must dissect the terminology. Legally speaking, a "residence post office address" is the place where a person actually physically resides. If you are on the move and do not possess a home in South Dakota, this applies to you.

The statement of "the address I have provided with my South Dakota Application for Title and Registration is strictly for mail-forwarding purposes" provides a bit of legal coverage. It clearly claims that you do not reside at the address provided (PMB), and that it is only used for mail collection. You must complete this affidavit and have it notarized locally.

Next is the application for your new title and registration. This is a lengthy form, and will need to be very precise. This form will transfer your current title from the state you will be leaving to a South Dakota title, and will generate your new license plates for the vehicle. The following explanations should help you choose the appropriate content for this form, which is displayed in a couple of pages.

Section I: This will likely be the first option of Transfer-New-Out-of-State. This notifies the state that you are bringing your title from your previous state into theirs. The optional Brand section is likely inapplicable.

Section II: This should be blank, as you do not have a title yet.

Section III: This is the exact information which will appear on your title and registration. This must be precise. You only need to complete one line in the first section.

Owner/Lessor/Trust: The name of your trust for the vehicle. This is exactly what will appear on the title and the registration. I prefer to use a generic title, such as The Motor Vehicle #728495735423001118720438-A Trust. This specific length of a trust title will be explained later. This may be a trust where you are the trustee and grantor, as explained previously.

Type of Ownership: Trust

Customer Type: Trust

Identification #: This should be your SSN. Before you grimace at this, let me explain. This scenario is the second option discussed in this chapter. As mentioned previously, each option adds additional privacy protection. In this example, your name is already attached to your vehicle, there is a strong history of this publicly available, and you are convincing the state that

YOUR trust is the new owner. You will need to send a copy of your SSN card or a tax statement, such as a 1099, as proof of SSN, along with this form. Any state will demand to know the name and identifiers of someone associated with the trust. This allows them to track down a responsible party if something illegal occurs or tickets are not paid. The rest of the options in this window can be left blank.

Owner/Lessor/Trust Mailing Address: This should be your PMB address.

Owner/Lessor/Trust Physical Address: This should be your PMB address.

Lessee/Trustee Mailing Address: This should be your PMB address.

Lessee/Trustee Physical Address: This should be your PMB address.

Section IV: Enter the VIN, Make, Model, Body Type, and all other details exactly as they appear on the current title. The odometer reading should be accurate as of the date of completion. The Dealer Price and Trade-in areas can state "Not Applicable".

Section V: Check the Tax-Exempt box and enter 18 as the code if you have already paid sales tax on the vehicle through another state. This code will be explained later. In this section after "3", enter the date the vehicle was purchased from your original bill of sale. Provide the additional sales price and tax details as obtained from your bill of sale or original title application. Assuming you originally paid at least 4% sales tax at the time of purchase, or when registering within your original state, you will not owe any taxes.

If you purchased the vehicle in a state without sales tax, such as Oregon, you will need to pay the appropriate taxes on the vehicle (4%). Overall, most states have a higher vehicle sales tax than 4%. If you purchased from a dealership, you are likely already covered. For most people, the minimum title fee of $10 will be appropriate.

I strongly encourage you to inspect the final page at the end of this form. There are many scenarios where a used vehicle is automatically tax-exempt, such as being at least 11 years of age and sold for less than $2,500. Before submitting this form, be sure you understand each section. There are many support documents on the state website.

Section VI: If you do not have a lien on the vehicle, this can be blank.

Section VII: If you do not have a lien on the vehicle, this can be blank.

After you have completed all of the forms and gathered your certification of trust, copy of your SSN card, and previous vehicle title/bill of sale, you need to determine the amount you will owe for the registration plates. South Dakota operates on a calendar year, and your renewal date will vary based on the name of the trust and the current month. Instead of trying to work out the details, I recommend calling the DMV and asking them to tell you the fees. A full year renewal is approximately $50-$100, so this prorated amount should be less. You can also take this opportunity to tell them everything you have done and ask if there is anything you are missing. Books can become outdated and state policies can change. Never complete these steps without verifying everything with the state. The staff have been surprisingly helpful during my calls.

Earlier in this chapter, I explained that a lengthy trust name, such as The Motor Vehicle #728495735423001118720438-A Trust, could be valuable for privacy protection. In this scenario, you have provided your real name and SSN to the state. YOU are the trustee of your own trust. We accept this because of your previous history with the vehicle. We still do not want your name on the title or the registration. While we only stated the trust name on the form, you provided a copy of required identification, specifically your SSN card. You also provided your certificate of trust identifying you as the trustee. Your name is not on the application, but it is on the card and this document. In my experience, most employees will only place the trust name on the title and registration, but some employees may go the extra mile and add your name to the registration. If you chose a name of trust similar to the above, the title could appear in one of many ways, such as the following.

The Motor Vehicle #728495735423001118720438-A Trust
The Motor Vehicle #728495735423001118720438-A Trust, John Doe, Trustee
The Motor Vehicle #728495735423001118720438-A Trust, John Doe, TTEE

There is only room for a set number of characters on the title and registration. This number fluctuates, but it is very likely that your title may display only the following.

The Motor Vehicle #72849573542300111872

In other words, a lengthy trust title might prevent your name from appearing on various databases that receive vehicle registration data from the state. South Dakota does not aggressively share their data as much as states such as California and Illinois, but you must always expect any information to eventually become public.

Date: **State of South Dakota Application for Motor Vehicle Title & Registration**

I. This application is for (Check one only)	Brand (Check if Applicable)	II. South Dakota Title Number
Transfer - New - Out-of-State ☐	Manufacturer Buy Back ☐ Rebuilt ☐ Junking Certificate ☐	
Interstate ☐ Operation by Law ☐	Manufacturer Buy Back - Rebuilt ☐ Salvage Total Loss ☐	
Repossession ☐ Unpaid Repair Bill ☐	Manufacturer Buy Back - Salvage ☐ Recovered Theft ☐	Title County Number
Abandoned ☐	Manufacturer Buy Back - Junking Certificate ☐ Parts Only ☐	

III. 1-4 Owner's/Lessors's/Trust's Name (First, Middle, Last), Description of type of Ownership (and, or, DBA, WROS, Guardianship, lessee, lessor, trustee etc.). Identification Number (SD Dr. Lic., SD ID, Soc. Sec. No. Fed Emp. ID. No.), Description of Customer Type (Individual, Company, Dealer, Government, Trust).

Owner/Lessor/Trust	Type of Ownership	Customer Type	Identification # (SD DL, SD ID, SSN, FEIN)
Owner/Lessee/Trustee	Type of Ownership	Customer Type	Identification # (SD DL, SD ID, SSN, FEIN)
Owner/Lessee/Trustee	Type of Ownership	Customer Type	Identification # (SD DL, SD ID, SSN, FEIN)
Owner/Lessee/Trustee	Type of Ownership	Customer Type	Identification # (SD DL, SD ID, SSN, FEIN)

ADDRESS See Special Mailing Address in Section VII				
	Owner/Lessor/Trust Mailing Address	City	State	Zip Code
	Owner/Lessor/Trust Physical Address (Residence Post Office Address)	City	State	Zip Code
	Lessee/Trustee Mailing Address	City	State	Zip Code
	Lessee/Trustee Physical Address (Residence Post Office Address)	City	State	Zip Code

IV. Primary VIN or Serial Number:

Make	Model	Body Type	Vehicle Code	Year	Weight/CC	Color	Fuel	Previous State/Brand

Secondary VIN or Serial Number: **Year:** **Make:**

Odometer Reading (Complete for vehicles 9 years old or newer): **Units** (Check one): Miles ☐ Kilometers ☐

Odometer Brand (Check one): Actual Mileage ☐ Exceeds Odometer's Mechanical Limits ☐ Not Actual Mileage ☐

Dealer Price Certification: I hereby certify that the purchase price and trade-in allowance in Item V. of the application is correct and that all accessories and added equipment have been reported.

Dealer Name and Number	Signature of Dealer or Dealer's Agent	Dealer Sold Permit

1st Trade-In **2nd Trade-In**

Year	Make	Serial No.	SD Title No.	Year	Make	Serial No.	SD Title No.

V. Motor Vehicle Purchaser's Certificate **(Note: A guide published by the automobile industry will be used to check values)**

1. Tax Exempt
(If claiming exemption, list exemption #) _____
Rental Vehicle/SD Sales Tax # _____
Non-Profit Donated Vehicle/Corporation #

2. Title Only (If applying for a "Title Only," in signing this application you are attesting that the vehicle will not be used upon the streets and highways of this state or any state. Application must be made within 45 days of purchase date.	**VI. Important: Electronic Lien & Title - A paper title is not issued until lien(s) released or upon request by lienholder for other approved purpose.**
3. Purchase Date	**1st Lienholder:**
4. Purchase Price (see Reverse Side) Bill of Sale Not Available Computer NADA'ED	Mailing Address:
5. Less Trade-In Allowance	City/State/Zip Code:
6. Difference	**2nd Lienholder:**
7. Tax 4% of Line 6, Snowmobile 3%	Mailing Address:
8. Tax Penalty & Interest	City/State/Zip Code
9. Credit for Tax Paid to Another State	To add additional lienholders, see section XI on reverse side
10. Title Fee	**VII. Special Mailing Address: (If other than owner/lessor address)**
11. Late Fee (Application made after 30 days)	Name:
12. Lien Fee	Address:
13. Balance Due for Title Application	City/State/Zip Code:

The applicant, under penalties of law and as rightful owner of the vehicle described on this application, declares that the information set forth on this application is true and correct.

PENALTY: Any person failing to pay the full amount of excise tax is subject to a Class 1 misdemeanor.

PENALTY: Any person who intentionally falsifies information on this application is guilty of a Class 6 felony.

MV-608 (05/12)

Signature Date

Signature Date

The next document is the tax payment verification form. This formality prevents you from paying vehicle taxes on a used vehicle that has already had proper taxing applied. In your situation, you may have purchased a new or used vehicle many years prior, and are transferring the title to a new state. South Dakota now wants to receive the appropriate sales tax on that vehicle, especially if it has a new owner. Unlike tax-hungry states such as California, the nomad-friendly states of South Dakota and Texas have waivers to prevent double-taxation. In the original bill of sale for this vehicle, the taxes paid should be clearly defined. That information is used to complete the form, and the taxes paid are applied to South Dakota's tax requirements. As long as the percentage of taxes originally paid meets or exceeds South Dakota's vehicle tax rate, there will be no tax due. The following is an example of this form, SD 1731.

South Dakota
Division of Motor Vehicles
Applicant's Tax Payment Verification

This form must accompany South Dakota's application for title to qualify for credit against South Dakota's motor vehicle excise tax for a like or similar tax paid to another state on the purchase of a vehicle. The out-of-state title being surrendered must be in the same name as the applicant. The applicant receives credit for the percentage of tax paid that is equal to or greater than the tax owed to this state

Name

_____

Street _____ City _____ State _____ Zip _____

Amount Paid _____ Tax Type _____ Sales tax was paid to _____

Date of payment _____

This statement is made with the knowledge that it is a Class 5 Felony to make a false statement and that in doing so, I am subject to the penalty of South Dakota law.

_____ _____

Applicant's Signature Date

The final document is the South Dakota Exemptions form which is only required if your previous title was in your real name and you want the new title to reflect your trust name. This is a powerful step in this process. It is quite easy to transfer the title from one state to another if the owner information remains identical. Since we are changing the name of the owner (from you to your trust), we must request a waiver of vehicle sales tax.

The previous form explained to the state that taxes have already been paid on this vehicle and waives the need to pay them again. That only applies to the original owner who paid those taxes (you). If you had sold this vehicle, the state would want a vehicle sales tax from the new owner. Transferring from your name to the trust name has the appearance of a new owner. Therefore, this form will request to waive the taxes since you are technically still the owner.

Since you do not possess a title number yet, leave the first field blank. Supply the odometer reading on the vehicle (miles), and place "NONE" in the lien holder field. The tax exemption code, which was also provided within the application, should be 18. The following is the explanation for this code.

18. Motor vehicle/boat transferred by a trustor to his trustee or from a trustee to a beneficiary of a trust.

This summary is not exactly your scenario, but it is the only option on this form acknowledging a trust. Technically, you are a trustor transferring to the TRUST. I have spoken with numerous employees of the South Dakota Division of Motor Vehicles over several years about this. They have all agreed that this exemption is appropriate for the purpose of transferring a vehicle from an owner into a trust created by that same owner.

Include a certification of trust as explained in the previous chapter with all of these forms. By including this document, you satisfy any concern from the state that you are associated with the trust as the previous owner of the vehicle. This ties everything together.

Obviously, South Dakota knows that you own the vehicle and you are associated with the trust. This is acceptable since the vehicle was already titled in your name previously. The title and registration will (hopefully) not display your name, and will only disclose the trust name. If someone queries your license plate, South Dakota will only display the trust name. This is why I encourage clients to never use the same trust for a vehicle as they would use for a home. Isolation between the two are vital. This is also why I encourage clients to never use a LIVING TRUST for a vehicle purchase. If the police need to contact you in reference to a traffic investigation, they can contact the state DMV to identify the grantor of the trust (you).

SOUTH DAKOTA EXEMPTIONS

This form is to be used when claiming an exemption from the South Dakota excise tax on a South Dakota titled vehicle/boat.

South Dakota Title Number _____

Odometer Reading is_____which is actual vehicle mileage

1st Lien holder _____

Mailing Address _____

City _____ State _____ Zip _____

_____ Tax Exemption being claimed (indicate number)

BY SIGNING THIS FORM YOU ARE ATTESTING THAT THE EXEMPTION BEING CLAIMED HEREON IS TRUE AND CORRECT. ANY PERSON WHO INTENTIONALLY FALSIFIES INFORMATION ON THIS FORM IS GUILTY OF A CLASS 6 FELONY.

_____ _____

Signature Date

Let's catch our breath here and summarize a few things. In the first scenario, you own a vehicle in the state you physically reside. It is registered in your real name and you want a thin layer of protection by re-titling it in the name of a trust created specifically for this purpose. YOU are the trustee of the trust, and you can complete all required paperwork from your state. You are still associated with the vehicle, the state knows who you are, but your name is no longer captured by intrusive plate scanners that are becoming common in many areas of the country. This is a small step.

In the second scenario, you are leaving your current state and PLAN to become a nomad in South Dakota. Within 45 days of obtaining your PMB, you title and register your vehicle with the state. You have a trust where YOU are the trustee. You submit the application to title the vehicle in the trust name, and you provide valid proof that you have this authority (certificate of trust). You explain that you already paid the taxes on this vehicle within another state and request waiver of any additional taxes. South Dakota knows you are associated with the vehicle, but your name is not likely displayed on the title or registration. As in the previous option, your name is not collected by vehicle scanners or nosey neighbors with friends in law enforcement. If a police officer needs to identify you, he or she can do so through the state DMV, but not through a traditional license plate check from within the patrol car.

In both of these scenarios, your home address is no longer publicly associated with your vehicle registration. You either used a PO Box (first scenario) or a PMB (second scenario). The PMB affords more protection because it is not likely near your home. When you are involved in a vehicle crash, and the officer copies the address from your vehicle registration onto the report, it will not be your home. These reports are public property, and anyone can obtain a copy.

I should pause here and give the obligatory warnings. Never lie on any government document. This will bring more attention and kill any decent shot at achieving privacy. Only use the nomad route if you plan on eventually executing full nomad status. This includes leaving your old state behind. If you live in Illinois and order plates from South Dakota, you cannot simply continue to live and work in Illinois while driving your newly registered vehicle. This violates the laws of Illinois (or any other state). Nomad status is for those that desire to travel and will not spend over 50% of a given year within a single state. South Dakota registration allows you to travel in your vehicle within any state, but abusing this privilege will bring unwanted attention.

Next, we take things to the next level with a new or used vehicle purchase. In these scenarios, the vehicle has never been associated with your true name, and there is no history within any database. Much of the process will be the same, but you will no longer be the trustee.

New Vehicle Purchase Through a Trust (Non-Nomad)

Next, assume you are NOT a legal nomad and will be buying a new vehicle. You do not want it associated with your name at any point. This will require a nominee. Any new vehicle purchase and registration must be attached to an individual at some point, and both the dealership and the state will demand identification from the purchaser. This applies even if paying with cash. Consider the following, which was recreated from my notes after a client purchase in 2018.

My client, whom I will refer to as Jane, wanted to purchase a vehicle anonymously. She is somewhat famous, and does not want her name publicly associated with the vehicle in any way. She is not a "nomad" and has no desire to go down that route. She has the cash to purchase the vehicle, but knows the dealership will be invasive in regard to her privacy. She desires an upscale vehicle with a hefty price, but the actions here would apply to any new vehicle purchase with cash. She identified the exact make and model she desired, and I approached the dealership.

I advised that I was representing a private buyer that already knows the vehicle she desires, which is currently on the lot. Jane was not concerned with bargaining, and accepted the typical purchase incentives, which were likely overpriced. When you shop for a vehicle, I recommend visiting several dealerships and obtaining "best offer" quotes from each. Use these to force lower prices from competing dealers. It is a difficult game.

I advised the dealer that I had cash in the form of a cashier's check which would be presented at the time of purchase, and could be confirmed with the local issuing bank. I also clearly stated that the vehicle would be placed into a trust and that the trustee of the trust would sign all necessary documents. Jane had already established a trust, as explained previously, and chose a standard grantor style trust with a close family friend assigned the role of trustee. The sales person started creating the necessary paperwork, which is when I encountered the first issue.

The dealership demanded government identification from the trustee. They stated this was due to money laundering and other financial crimes, and it was a requirement from the state. I advised that I could definitely comply with this, but that I would need a copy of the state or federal law demanding this for cash purchases. In my experience, many dealers know the law and present me with the Specially Designated Nationals (SDN) List provided by the Department of the Treasury, which the dealership is mandated by law to check during each purchase. The SDN List is comprised of "individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries". It also lists "individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific". Surprisingly, this list is publicly available at the following address.

https://www.treasury.gov/ofac/downloads/sdnlist.pdf

In approximately 25% of my dealer interactions, they do not know why they are legally required to check identification and tell me not to worry about it. I present more detail on this, including defenses against it, later in this chapter.

When buying from a dealership which obeys the law, there is no way around this requirement. While some dealers may "forget" to check in order to make the sale, I have encountered many that were willing to let me walk out of the door, losing the sale. Fortunately, acceptable identification for this purpose is not very demanding. I have shown passports, SSN cards, and in one scenario a library card. Your mileage may vary. For Jane's purchase, I displayed a photocopy of the passport of her trustee to the sales person for verification. This is invasive, but does not expose Jane. I refused to allow the dealership to copy it citing the following federal law.

"18 U.S. Code § 1543 - Whoever … furnishes to another … a passport… Shall be fined under this title, imprisoned not more than 25 years.

The above words are verbatim from the federal law for "Forgery or false use of passport". I left out a few words, and the entire section appears as follows.

"Whoever falsely makes, forges, counterfeits, mutilates, or alters any passport or instrument purporting to be a passport, with intent that the same may be used; or Whoever willfully and knowingly uses, or attempts to use, or furnishes to another for use any such false, forged, counterfeited, mutilated, or altered passport or instrument purporting to be a passport, or any passport validly issued which has become void by the occurrence of any condition therein prescribed invalidating the same-Shall be fined under this title, imprisoned not more than 25 years.

The full version makes it clear that there must be an attempt to commit fraud in order for this law to apply. My redacted version sounds much more concerning to the dealer. The law requiring dealers to check identification does not require them to maintain a copy of the identification. This is often an awkward moment, but I refuse to allow a car dealership to maintain a copy of a government issued photo identification of me or any client. If I were replicating this today, I would cite 18 U.S. Code 701, which is verbatim as follows.

"Whoever manufactures, sells, or possesses any badge, identification card, or other insignia, of the design prescribed by the head of any department or agency of the United States for use by any officer or employee thereof, or any colorable imitation thereof, or photographs, prints, or in any other manner makes or executes any engraving, photograph, print, or impression in the likeness of any such badge, identification card, or other insignia, or any colorable imitation

thereof, except as authorized under regulations made pursuant to law, shall be fined under this title or imprisoned not more than six months, or both."

I believe that TECHNICALLY this law makes photocopies of government identification cards unlawful. This was not the intent, but car dealerships do not usually have legal teams on site to debate this. The wording is much cleaner than the previous example. I always encourage sales people to Google the code and see for themselves. I will revisit this law later when we tackle companies who constantly wish to copy or scan your identification, such as casinos, clubs, concert venues, and pharmacies.

I furnished a copy of the Certificate of Trust, which was signed by the trustee and notarized. This satisfies the requirement for the bill of sale and eventual registration. I advised that I desired the dealership to complete the vehicle registration documents and submit them to the state. The final invoice would include these charges. I only request this when purchasing via a trust within a non-nomad state as a non-nomad. I will explain a better option for nomads in a moment in which I would never allow a dealership to submit my paperwork to the state.

I have found that allowing the dealership to apply for title and registration in this specific situation results in much less scrutiny. When a dealer submits dozens of title requests, they are approved almost instantly. When you or I submit an application, it is scrutinized to make sure we did not make any mistakes. This is especially true when titling to a trust. Many states only offer standard applications that insist that the vehicle be registered to a full name and physical address. Often, dealerships know of more appropriate forms that allow the use of trusts and LLCs.

I always ask to see the application before it is submitted. I expect to see the trustee's name on the application, but I want to make sure the name is not included on the line which displays the title of the trust. We are always at the mercy of the DMV on how it is officially entered. Regardless, the dealership has never known the name of my client, so I never expect to see any concerning exposure.

The address of the trust for the title and registration will vary. Many states will accept a PO Box if you can confirm you receive mail through it. Of those that refuse, some allow the use of a UPS or other CMRA address. Some states enforce a policy of providing an actual physical address. If you do not have a business address or other option, you will be forced to register to your home address. I dislike this option, and I encourage you to find a legal address to use that shares the least amount of personal information while obeying the law. Law enforcement readers may scoff at my opinions on this. I understand. As a retired LEO, I respect the need to track down a criminal after a license plate is identified. You still have this power, but it may take a couple of additional queries. If data mining companies, license plate scanners, and other

invasive entities were not collecting and sharing this data daily, I would not feel so inclined to protect our name and home address from appearing on a vehicle's registration.

At some point, the dealership will need a signature from the trustee. If your trustee is local, this is best achieved in person at the dealership. If not, the final documents can be shipped to the trustee, signed and notarized, and shipped back. In my scenario, the trustee was able to respond to the dealership and sign the final paperwork.

Jane now possesses her new car. It is titled and registered to her trust, and her trustee is identified on the paperwork with the state. Jane's name is not mentioned anywhere. The address is a UPS box which Jane owns. If Jane commits a hit-and-run, law enforcement will know her UPS address and her trustee's information. Contacting the UPS store or the Postal Service will identify Jane through her USPS form submitted to UPS. Contacting the trustee will provide another lead. She does not have a free pass to be irresponsible.

I can't stress enough that your mileage will vary with this. Every state has its own nuances and policies. Each employee at the DMV may have his or her own opinion on the rules. I only hope that these sections provide some insight into your options. Next, I present the most private execution.

I highly recommend that you always have a back-story memorized for the dealership. As soon as a salesperson meets you, he or she will be inquisitive. They will either be polite, pushy, obnoxious, or arrogant. They are trained to generate small talk in order to make you more comfortable. They will push you for small details which they will use during price negotiation. If they discover that you have kids, they might push extra safety features and services. If they find out you are single, they may push you toward sportier models. I avoid all of this within the first few minutes with the following dialogue.

"Thank you for your time, I am sure your value each hour as much as I do. I don't plan to waste your day. I have cash to buy a vehicle, I know what I want, and I purchase several vehicles yearly. I am not one for small talk, and I do not hear very well. Therefore, please forgive me if you feel ignored. I simply want to focus on my hunt for a vehicle. Can you please show me the various [insert make, model, and trim package] which you have on the lot? I am purchasing on behalf of a trust, and I have very specific features and pricing which I must accommodate. If you have something which meets my criteria, I can purchase today. The trust beneficiaries are very sensitive to queries about their wealth, so I prefer to keep their information private. I can provide full payment today via cashier's check, and I can provide a proof of funds letter from the bank if you wish. That all being said, let's go pick out that car!"

This almost always results in an enthusiastic sales person ready to complete a sale.

New Vehicle Purchase Through a Trust (Nomad)

Finally, assume you are a legal nomad of South Dakota and you wish to purchase a new vehicle privately. You already have your South Dakota driver's license, and the state is your official domicile. You are in a perfect position to take advantage of several layers of privacy from the public. This section will replicate many of the previously mentioned tactics, so I will keep this abbreviated.

Obviously, the first step is to identify the vehicle you want. This can be from a dealership or a private seller. Having the dealer complete all of the paperwork is always easier, but submitting your own registration application is not difficult. The details were explained previously. The state of purchase should not matter with a few exceptions. Regardless of where you purchase the vehicle, you will owe sales tax to South Dakota. The exception is California. If you purchase a car there, you must pay the inflated California taxes, which will be more than twice the South Dakota tax. South Dakota will not "double tax" you, and allows you to claim any previous state tax paid. Most states will not tax the vehicle purchase, as you will be paying the vehicle tax when you register and title the vehicle. If you buy from an individual, you will pay the taxes at the time of registration.

Let's assume you are purchasing from a dealership. You will provide your Certificate of Trust identifying the trust name and name of your trustee (not you). This trustee has the powers to sign on behalf of the trust, but will need to disclose their SSN to the state. This can be very invasive, so make sure you have a trustee willing to participate at this level. You will declare that you will be registering the vehicle in the name of the trust in South Dakota. The address used will be your PMB, and the PMB is already prepared to accept mail in the trust name. The dealer will complete the title application on your behalf and determine the amount owed to South Dakota for taxes and registration. The other documents completed previously are not required because you have established domicile and are not requesting a waiver of taxes. Your trustee will sign the paperwork and you will pay in cash via cashier's check. The process should be fairly painless. If buying from an individual, you will complete the application for title as previously explained. It is the only document you need. The only difference is that you must pay taxes on the new (used) vehicle.

You are responsible for the vehicle and its usage. It is legally registered for use anywhere in the country. If you misbehave, your license plate leads back to your trust name at your PMB. Law enforcement can quickly identify you and your trustee. However, public databases will only know the trust name and PMB address. Neither expose your home address. Querying the plate through a public or government database will not reveal your name. I have oversimplified the details and benefits, but the previous pages in this chapter have already explained the overall process.

New Vehicle Purchase Through an LLC

You likely noticed that none of my previous scenarios included titling the vehicle to an LLC. There are two main reasons why LLC ownership of a vehicle is not appropriate for many of my clients, especially if they reside in states with no respect for privacy. In a moment, I explain my current preferred method of vehicle ownership, but let's first consider some complications.

Insurance: Many insurance companies refuse to insure a vehicle titled only to an LLC. Those that allow this demand premiums that are sometimes twice or triple the personal rates. The insurance companies will still want to know the primary policy holder and might demand to see your operating agreement identifying the members of the LLC. Most will demand that any vehicles titled in the name of an LLC includes the member information on the registration.

State requirements: Some states require disclosure of all LLC members if you register a vehicle to the business. Many states require out-of-state LLCs to file as a foreign entity within the state of registration. In other words, if you live in California and purchased a New Mexico LLC, you must register the LLC in California before a vehicle can be titled. This registration must include the names of all members (and an $800 annual fee). This violates the privacy of a New Mexico LLC.

Titling vehicles that are used for business purposes to an LLC is acceptable, but that is outside of the scope of this book. Some will argue that a New Mexico LLC is the most private option since the state does not know anything about the members of the LLC. This is true, but the state where you register the vehicle will still likely demand to know a person's name who is associated with the LLC. The application for registration must be signed by someone, and that person will need to be identified. I have previously registered personal vehicles in a New Mexico LLC. Today, the privacy protection is much more limited.

If you choose to register your vehicle in the name of an LLC in your state, almost all of the previous instruction applies. You will need to provide the LLC documents, complete the title application, and sign on behalf of the LLC. If you use a nominee, that person must be included in your LLC documents, which can complicate matters quickly. A trustee can be easily replaced on a trust. Removal of a member of an LLC can require votes and amended agreements.

In past years I have had great respect for registering vehicles into New Mexico LLCs. I believe most states have caught on to this loophole and have taken measures to require additional details about the person. It is absolutely still possible to register a vehicle to an anonymous LLC in some states. However, these opportunities are disappearing rapidly. The stigma of LLCs as a way to hide assets have damaged this practice. The use of a trust seems to be more widely accepted as legitimate behavior. However, there is one last option, which has proven to be the most beneficial strategy for my clients over the past year.

New Vehicle Purchase Through an LLC (Nomad)

Your most privacy-respecting option for a vehicle purchase and registration occurs as a nomad with an LLC registered through your domicile. This strategy combines numerous lessons which have already been explained, and eliminates most hurdles we have observed with the previous options. I explain the entire process through an actual client example from late 2019. This revisits some of the content already presented in this chapter, but I believe it helps summarize the overall ideas. Meet Jen Doe.

Jen reached out to me after I had previously helped her disappear as a nomad in South Dakota. She had already established her new life, lived in an anonymous home, and needed a new vehicle. She insisted that the purchase be made in cash and that neither her name nor SSN be present on any paperwork. Furthermore, she demanded that no SSNs be used throughout the process. She possessed the funds necessary for the type of vehicle she desired, and had already chosen a make, model, and color of her next car. She was not in a huge rush, and asked me to complete the entire process on her behalf the next time I was near her area. Jen was one of my first clients to complete the program, and I was eager to tackle this issue. I had some new ideas to test since the first version of this book, and she was eager to be my test case. Within a month, I was at her doorstep, and I was not empty-handed.

I had established her South Dakota LLC which would be used for the purchase. She was already a nomad resident of the state, possessed a driver's license, and a PMB. I formed the LLC under a random business name on her behalf and opened a new PMB address for the business under her name (with her consent and assistance). All of this was completed online, and the digital LLC paperwork was generated immediately. The PMB provider knows the true identity of the box holder, but will not release this without a court order. I hired my friend with a common name to act as the "Organizer" of the LLC. The PMB provided an individual to act as the registered agent for the business. If the LLC were to be sued, the registered agent would receive the notice. He would contact her and deliver any court orders. Only my organizer's name, the registered agent, and the PMB address will be publicly accessible.

I gave her all of the LLC paperwork and we created her supporting documents as explained previously. The LLC was now legally hers, and I was contracted to maintain the PMB and registered agent service. Neither her name nor mine is publicly associated with the LLC. A subpoena to the registered agent could identify her, but this is not a concern to me. We obtained an EIN from the IRS, which is mandatory for this protocol. The EIN is associated with her SSN, but this is not public information. She may be required to include this EIN in her annual tax filing, but there will be no income and no taxes due. The IRS provided immediate verification of the EIN and a physical letter soon followed. All of the LLC paperwork was in place. While not completely anonymous, she had a legal business infrastructure which could not be publicly connected to her. We were ready to go shopping.

It was now time to test the local dealers. I refer to this as my "Test Drive Test". I find a local dealer from which I have no desire to purchase, and where I can test drive a couple of vehicles. I start asking questions about their purchase demands, such as ID requirements and payment options. I have found that dealers from various states and metropolitan areas possess different requirements. The only consistency is that most dealers in a specific area usually have the same procedures. As an example, every dealer I have encountered in Los Angeles requires a valid unredacted government photo ID and electronic wire for cash purchases, while dealers in less-populated areas accept redacted identification and personal checks. I learned quickly that this dealer absolutely required photo ID and SSN, but had no payment preference.

Now that I had some basic information about the dealers in the area, it was time to contact the desired dealership. It is important to engage in several conversations via telephone and email before ever responding to a dealer. When you show up "cold", you are randomly assigned to the first sales person who has the free time. You will be brought directly to a desk and asked for ID. You may spend an hour at the dealership before you ever enter a vehicle. This is unacceptable to me. Therefore, I avoid drop-ins altogether. Instead, I begin the conversation with a call.

When I contact a dealership via telephone, I request to speak with the commercial fleet sales division. If the dealer does not have a dedicated commercial sales representative, I move on to another place. This is vital for my protocol. Commercial sales departments are less restrictive on purchase requirements such as ID and electronic payments. Also, they are less pushy in regard to sales. These dealership employees deal exclusively with companies purchasing vehicles as part of a larger fleet. The buyer of the vehicle is usually not the owner of title or source of payment. Think of the person who buys vehicles on behalf of a taxi service. His or her name is not included on the check or receipt. They are simply the employee assigned to purchase vehicles. While on a much smaller scale, I play that role.

My first call explains that I represent a business which wishes to purchase at least one vehicle. I specify the exact make and model, and ask what availability is currently present on the lot. I then request detailed final pricing for fleet account purchase be sent to my email. I already have an official address ready, such as fleet@myLLC.com. This is never the best price, but a decent negotiation starting point. By opening with an audio call and transferring the conversation to email, I have established a rapport with the sales person. I continue the conversation remotely and start negotiating a final price. This demonstrates my clear intent to purchase a vehicle, and the dealer knows that I do not need multiple test drives and time to contemplate the purchase. I want to convey that I am a serious buyer ready to complete the purchase. This rapport will provide numerous benefits in a moment.

In this scenario, I had established a good relationship with a commercial sales representative, and he stated that he had the exact vehicle desired. He offered to have it detailed and ready

for inspection. I agreed to respond to the dealership at 2 pm on the next day. At 2 pm, I sent a text message to his cell phone to report that I was running late, but would be there that day. This is very intentional. When a sales person has a potential purchase scheduled, he or she has a routine prepared. This may include sitting at their desk to review paperwork or the dreaded meeting with the sales manager. Both scenarios introduce the opportunity for invasive demands such as copying my identification or providing a cellular number to them.

Instead, I showed up at 3 pm. I walked in, advised the receptionist that I had arrived, and asked her to let my sales person know I would be out in the lot looking at the fleet. This is also intentional, as it moves the first face-to-face meeting on more neutral territory. It is hard to complete paperwork, make copies of IDs, or meet the manager while we are outside on the lot. If I am feeling aggressive, I will advise the receptionist to have keys to the vehicle brought out. I then immediately walk toward the lot before a response can be given. Car sales people simply want to sell cars. The more confidence I portray, the more I can control the environment. In this scenario, my sales person practically ran out to meet me at the vehicle he had ready at the entrance. He had keys in hand, introduced himself, and opened the vehicle doors in order for me to inspect everything.

The test drive was not very important, but I decided to sell the role I was playing. Since I had already given him an alias name, a number he believed was my cell, and a business email address matching the name of my LLC, there was very little scrutiny. I was never asked for a copy of my license before the test drive. However, I had already disclosed the LLC name, EIN, and address details via email. This will all be required for the final paperwork, and providing it in advance creates a sense of trust from the sales person. I drove the car, confirmed the vehicle and the negotiated price were acceptable, and asked how he preferred payment. I was now ready to start the paperwork.

We returned to his office and he began asking for information. He pulled up my "lead" in his computer, which is an entry within his database for sales leads. I asked to look at it, and he obliged. It displayed my alias name, VOIP telephone number, and the name and address of the LLC. I was more interested in the portion of the screen which displayed my text message telling him I was running late. Sales people also use VOIP numbers, and rarely distribute their true cellular number. This leads system identified the VOIP number assigned to him, and allowed him to review all emails, calls, and text messages exchanged with a potential client. This also means that my content was stored within this system and likely shared with third parties. I already suspected these scenarios, and I was not surprised.

I confirmed all of the business information and insisted that the vehicle be purchased in the business name. I also confirmed the EIN of the business, and ensured that it was provided any time his system requested an SSN. The sales person seemed familiar with the process of

purchasing a vehicle in a business name, and was not very invasive of my own information. However, we quickly reached a point of privacy concern once OFAC presented itself.

As stated previously, dealers must query all car buyers against a database of people who are blacklisted by the government. The U.S. Department of Treasury Office of Foreign Assets Control (OFAC) list of specially designated nationals and blocked persons is the database queried by car dealerships. The OFAC list identifies people who are sympathetic with or involved with foreign terrorist groups. Companies in the United States are prohibited from making a sale to anyone on the list. Car dealerships are more scrutinized than other types of businesses, and the government enforces this requirement more heavily on them. During the sale of a vehicle, a car dealer submits your name through the OFAC list, usually using specialized software. If the dealer gets a hit, they go through seven steps to try to verify the match. This is the first key point. Only a NAME must be submitted.

My sales representative asked to see a copy of my driver's license. From my experience, telling him that I was privacy conscious and refused to do so was not the best strategy. Questioning the need for my true name, address, DL number, and SSN is more likely to raise red flags. I already know that every dealership has a policy to demand government photo ID from every buyer and keep a photocopy on file. I have walked out of dealerships during the final cash-only sales agreement in previous attempts due to this demand. Instead, I stated "You are going to kill me, but I was so worried about bringing all of the appropriate business paperwork, that I forgot to grab my wallet. I can have another employee send over something if that works for you".

Remember my LLC organizer who has an extremely common name? I also hire him to remotely assist in these types of situations. I told my sales person that I could call my partner at the LLC and have him send over his ID. The sales person agreed, and I confirmed that he only needed to query a name. I told him that this employee was a little "weird" and becomes paranoid about identity theft. I stated that my employee would be emailing him a scan of his official government identification, with the image redacted. My organizer sent over a scan of his passport card, blocking out his photo. Since there is no SSN, address, or DL number visible on this ID, there was nothing else which needed redacted. The sales person looked a bit confused and concerned, and said he would need to speak to a manager to make sure this would suffice.

He stepped away for a few minutes and returned with his manager. The boss told me they would need a full DL with photo and an SSN in order to complete the sale. I questioned this demand with the following dialogue, which was discreetly captured with the voice recording application on my phone. For those concerned, I was inside a one-party recording state, which makes this legal.

"The sale is in the business name, and I have already provided the EIN for the business. Also, I have the letter from the IRS confirming the EIN as valid, which you can also confirm directly to them. I won't ask an employee to provide their SSN for a vehicle I am purchasing with business funds. Furthermore, I will not provide my own SSN because I am not seeking credit. The only way you would need an SSN is to conduct a credit check. I am paying in full with a money order, so there should be no credit check."

He started to blame OFAC, but I cut him off with the following.

"OFAC only requires a name and occasionally a DOB. If you get a positive hit on the name, it will then require additional information. At no time does it require an SSN, mostly because the vast majority of the list contains people outside the U.S. who do not have an SSN. If you can show me the SSN field on the direct OFAC submission, I will stand corrected. If you submit my employee's name as required by law, and receive a confirmed positive hit on that name, we are happy to comply with the additional requirements."

He had no desire to show me the OFAC submission, because he knew I was right. Dealers want an SSN in order to conduct a full credit check. Even when paying with cash, they will run your name and SSN to determine your credit score. They will then try to convince you to take advantage of their great financing offers. Why? Because they make a higher commission when you take a loan directly from the dealer financing.

The manager took the black-and-white print of the redacted passport card and had someone query the OFAC list. There was no hit. To be fair, there would be no hit on my name either. I know this because I have identified myself during previous transactions for other clients. He advised the sales person to continue with the paperwork. It was important to me to have this ID sent from a remote location. It is very difficult to tell someone in person that you do not want your photo copied. I do not trust covering the photo portion with something, as the person may remove the covering during the photocopy. By having it sent over remotely via email, any redaction is in my control. Also, if the copy comes from my "employee" with an official email address matching the domain which I used previously, my story appears more legitimate. Remember, we are paying in full with legitimate cash. There is no financial fraud taking place.

You may be questioning why I would allow anyone to send over an ID via email. First, there is no image present of my assistant. Second, his name and DOB can already be found through numerous public sources. There is no secret there. If this ID were to be leaked or breached, it would not have much value to the thief. It was scanned in poor quality and possesses no photo. If it were used to gain credit, it would not be accepted. Since no SSN is present, there is very minimal risk of fraud. Since the dealership never receives an SSN at all, this prevents accidental leakage or association with the ID.

I had successfully bypassed the demand to keep an unredacted driver's license and SSN on file with the sale. You may be a bit overwhelmed while reading this. You likely do not have an LLC organizer with a common name ready to stand in for you. I completely understand. I do not always take this aggressive route. In this scenario, my client insisted that my name was not involved. Most clients simply want their own name hidden from the sale. For most readers, I present the following alternative.

If you are purchasing the vehicle with cash in the name of an LLC with an EIN, there is not much risk in using your own name during purchase. The name you give to the dealer will not be used during registration with the state. It will likely only stay within their internal systems. However, I do encourage you to force them to redact your photo when they insist on making a copy. In episode 135 of my podcast, I include audio recordings of me delicately asking the sales person to properly redact my photo before making a copy, and allowing me to witness the copy being made. Remember, my DL has my PMB address, which is publicly available on people search sites. It does not expose my true home address or my SSN. It is much more vital to register the vehicle with the state in a business name than to worry about the dealer knowing your identity. Only you can choose the level of privacy desired. My strongest advice is to simply never provide your SSN during the sale. It will be abused.

Once we had moved past the awkward portion, it was time to begin the paperwork. This presents another dilemma. I will need to sign several pieces of paper. What name should I use? I made it very clear to the sales person that ONLY the LLC name should appear on any paperwork. This is fairly standard for commercial sales. Since I am authorized by the LLC owner (my client), I can sign any documents I desire. Remember, these are not government forms. These are documents from the dealership, which is a private company. Furthermore, my alias name never appeared within any documents. I was presented several documents and waivers, all of which only displayed the LLC name under the signature line. I scribbled an illegible signature on each. However, I scrutinized a few documents, as outlined below.

Dealerships have a standard packet used for every sale, even if some of the documents are not applicable. The first document I questioned was the "Credit Application". Although I was paying cash and required no financing, I was still asked to submit an application. I refused to sign, which was met with skepticism. I was assured by the sales person that my credit would not be checked. I believed him, as he did not have my name or SSN. However, I was concerned it may give them the authority to use my assistant's name and DOB to conduct a soft inquiry. I blamed a technicality which I observed within the document.

The SSN area of this application had "000-00-0000" as the SSN. This was because the system demanded an entry, but an SSN was never disclosed since the sale was made to an LLC. The last paragraph included "Everything I have stated within this application is true to the best of my knowledge". I informed the sales person that 000-00-0000 was not my SSN, and signing

this application with inaccurate data would violate the same document to which I was attesting. He agreed to waive this document.

Next was the credit bureau authorization document. Similar to the previous concern, this form provided consent to the dealer to execute inquires at Equifax, Experian, and TransUnion using any information provided. The only purpose of this query would be to authorize financing, which I did not need. The information included on this form was the LLC name and address. I advised that I did not have the proper authorization to consent to this. I further stated that the LLC would require a board meeting with two-thirds voting approval in order to authorize any credit inquiries or acceptance of credit terms, as clearly addressed in our legal operating agreement. This was not necessarily the case, but he does not know what is in our operating agreements. He agreed to waive this form.

Would it really matter if I signed these? Probably not. Remember, they do not possess any SSN number, which would be required in order to conduct a credit check. The EIN has no credit established, and an inquiry for credit would be declined. Even if you refuse to sign these consent forms, nothing stops them from proceeding anyway. This is why it is so important to never disclose an SSN.

The final document which I questioned was the Data Sharing Form. This paper identified the types of data which are shared with third parties, such as marketing companies. The default options display "yes" on everything, and the dealer hopes you willingly sign without reading. However, these documents almost always contain the exact paragraph as follows.

"Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do."

I then went through each line and questioned whether federal law allowed me to protect my information from being shared. "Can I limit sharing of my data for marketing purposes? How about from affiliates?" I found out very quickly that I could change most of the data sharing authorizations to "No". Will they share it anyway? Probably. However, I felt better about taking a stand against this practice.

The remainder of the paperwork was standard forms. The New Vehicle Delivery Checklist, Agreement to Provide Insurance, Delivery Sheet, Warranty Registration, and final sales contract all needed a scribbled signature, but all were only in the name of the LLC. The only document I was careful with was the Bill of Sale. The "closing manager" told me to sign under the LLC and write in "LLC Owner". I was not the owner any more, my client was. Therefore, I scribbled my signature and entered "LLC Representative". I don't think anyone noticed.

It was time to pay. I asked my sales person for the absolute final amount due, which he provided. I left, picked up the client (in her new car), went to a local branch of her bank, and had her issue a cashier's check in the amount due. This check obviously has a direct connection to her true account, but not one that can be publicly followed. The dealer cannot connect this check to her identity without a court order to the bank. We returned to the dealer, she waited in the car, and I issued the check to the sales office.

Surprisingly to me, most vehicle dealerships accept any type of check as full payment for vehicles. They will hold the title for up to two weeks while the check clears, so there is fairly minimal risk. If the check does not clear, I cannot receive the title and register the vehicle. Similarly, I can obtain credit for a vehicle but never make a payment. Either way, the dealership owns the vehicle until you make good on the full price. After the cashier's check clears, the Certificate of Origin will be mailed to the LLC PMB. We will use that later to title the vehicle and obtain registration plates.

This brings up another point. I never allow the dealership to register nomad LLC vehicles. In almost every scenario, they will make a mistake which could disclose the true owner during registration. It is possible that the dealer would disclose my alias name or my assistant's name to the state, which could then be considered fraud. I always insist that I will register the vehicle myself in this scenario. This usually makes sense if you are buying within a state outside of your PMB and LLC registration area.

This brings us to another issue. Can you buy a vehicle in one state and title it in another? Absolutely. My only exception to this is California. I would never buy a vehicle within that state if I was registering it elsewhere. This is because California dealers are required to charge full vehicle sales tax regardless of titling authority. This tax will likely be higher than what you would pay otherwise. In our scenario, assume I purchased the vehicle in Missouri. After advising the dealer that I owned a South Dakota LLC and would be titling the vehicle there, all sales tax was eliminated from the sale. I will need to pay South Dakota sales tax before the vehicle can be registered. I will explain more on that in a moment.

Let's take a moment to catch up. We purchased a vehicle at a dealership in the name of an LLC. The LLC is owned by my client, who is a South Dakota nomad. The LLC is registered in South Dakota without her name publicly visible in the online documents. The vehicle was purchased with funds from my client's bank account. By issuing a cashier's check, we eliminate anything publicly identifying my client. Her name and account number were not on the check. I signed for everything with a scribble, and my name did not appear on any documents. Only the LLC name was present, and I signed on behalf of the LLC with consent from the owner (my client). Technically, that was my real signature as Michael Bazzell. However, no name appeared anywhere.

Some may say that I committed fraud when I signed all of the paperwork. I disagree. If an alias name was present, and I signed as that alias name, then you may have a point. I entered into legally (civil) binding contracts. However, neither an alias or real name was ever present. I simply signed on behalf of the LLC, which I was authorized to do. Below every signature, only the LLC name appeared. My client, the owner of that LLC, authorized me to sign. If you were replicating this process with your own LLC, you could scribble anything you want over that line. No one can tell you how to sign your name. If it happens to be illegible, so be it. What is most important is that you have the authority to sign on behalf of the LLC. Once the dealership receives their money, they really do not care about much else.

We were allowed to leave with the vehicle. My client drove away in it while I entered my own rental. We possessed the vehicle, paid the full amount due, and never provided a true name of my client or myself. We had a couple of weeks to wait for the check to clear. My client contacted her insurance to tell them about the purchase, and make sure she had coverage under her name and the LLC. I explain more about insurance in a moment.

During the two-week wait, I was bombarded with unsolicited messages from the dealership and various affiliates. Although I clearly specified that they should not share my information, it was obvious that they had. The email address I provided to the sales person was used to register me into their daily spam program; the VOIP number I had provided began receiving text messages about vehicle-related specials; and the PMB received numerous brochures announcing upcoming sales and third-party services. This is why it is important to only use a burner VOIP number, a dedicated email address which can be ignored, and a PMB which can eliminate junk mail. None of this correspondence was connected to any important email accounts, telephone numbers, or physical addresses, so the privacy concerns were minimal.

After the check cleared, the Certificate of Origin was mailed to the PMB. This is a document from the vehicle manufacturer which is used to obtain a title. All of the vehicle details such as the VIN, are present and ready to be transferred to a title. The registration form for South Dakota was displayed previously in this chapter, and I used the same form for my nomad client. However, there were a few important differences. The first line in section three identified the LLC name, "Company" as the owner type, and the LLC EIN as the identification number. This EIN eliminates the need for any SSN or DL number on this application, which is a huge privacy benefit. I supplied the South Dakota PMB address and copied all vehicle details from the Certificate of Origin. Lines 4 through 14, which identifies the purchase price and taxes owed, were left blank. This is because there is a very low chance that your numbers will match the amount South Dakota believes you owe. Let me explain.

My client had not yet paid any sales tax on this vehicle. Since it will be titled in South Dakota, and because South Dakota is her domicile, they are owed the vehicle tax. This source of revenue for South Dakota provides several million dollars annually from nomad travelers, and

is a large reason that the state allows nomads to call it home. Like most states, the "sale price" is not the amount you gave the dealer for the vehicle. South Dakota ignores rebates, but pays attention to any extras such as dealer fees and delivery charges. You will pay tax on those. They basically look at your bill of sale and sales contract to determine the negotiated price of the vehicle plus any other expenses. That will be the basis of your tax, ignoring any rebates issued. This seems a bit unfair, but standard practice. Some states determine your tax owed based on the sticker price, which is ridiculous. Fortunately, the South Dakota vehicle tax is 4%, which is much less than most states.

The application had no names associated with it. The business name was the registrant, the business EIN was the identifier, and I scribbled a signature at the bottom. If the state department of motor vehicles wanted to track down an actual owner, they could identify the organizer of the LLC within their own records or contact the PMB provider and request owner information. There is a trail which could be followed, but the information is not publicly available. South Dakota is one of the most lenient states in regard to business registration of a vehicle. They do not need to ever receive any individual name.

I submitted the application along with a cover letter including an email address for contact once taxes were determined. I attached the original Certificate of Origin, bill of sale, IRS letter of EIN, and Certificate of Existence for the LLC. I sent everything via priority mail with tracking. Ten days later, I received an email from the South Dakota DMV notifying me of the tax owed on the vehicle. I called their office and paid the bill over the phone with a Privacy.com card created by my client. I received a 3% fee since I paid via credit card, but this resulted in only a $35 charge.

Two weeks later, her license plates arrived at the PMB and she had them forwarded to a nearby UPS store. She replaced the 60-day temporary tags provided by the dealer. The title arrived two weeks later and she now possesses a vehicle with proper title and registration. There is no public record associated with her name. She can renew the registration yearly through the state's website using a masked credit or debit card.

I want to stress again the importance of registering the vehicle yourself in this situation. I have had dealerships insist on providing this service because they will "make sure it is correct". I have seen those same dealers supply inaccurate details on the application. In one instance, the dealership attached a DL number on the registration form instead of the LLC EIN. Do not take any chances. Do it yourself and know that it was done right. The South Dakota DMV is surprisingly helpful when calling with questions. They are also well-versed in the needs of nomads. Never trust a PMB provider with this task. You will be disappointed in the result.

Insurance

I taught a 2-day privacy course at BlackHat in Las Vegas several years prior to writing this book. I discussed some of these techniques, and an audience member challenged me. He exclaimed that I was committing insurance fraud since my vehicle is registered and maintained in a state in which I am not present. He refused to truly listen to my response, but I hope you will allow me to explain why I disagree.

If you register a vehicle in South Dakota as a nomad, you must obtain insurance within South Dakota. I strongly advise contacting an insurance office within the county of your PMB address. They are much more familiar with the nomad lifestyle than a random office in another portion of the state. Your insurance provider will demand to know who YOU are (not your trustee or LLC name), as your rate and coverage is based on your credit score and insurance history. If you already have history of insurance coverage and a clean driving record, it will likely make the most sense to continue service with that provider. Assume you had Allstate coverage in Illinois. You recently left that state and now reside in South Dakota. Contacting an Allstate representative in South Dakota can be an easy transition.

When I contacted a local insurance representative in my state of domicile, and stated my PMB address, she immediately asked "Are you a nomad"? I made it very clear that I was, and that I travel often. I even went so far as to say that I am rarely in South Dakota, and neither is my vehicle. This was completely acceptable, as they have several members that are in the same situation. The insurance was transferred over instantly, and my rates decreased. I still have my full insurance coverage anywhere I travel.

The most important consideration with these scenarios is to ensure you have proper coverage. If your vehicle is titled into a trust or LLC, your insurance company must know this. More specifically, the trust or LLC must be listed as a "Secondary Insured" party. If you have an accident, and are sued, the lawsuit could be filed against you or your trust/LLC. You want the insurance company to cover both. I have never seen a price increase for this formality with a trust, but LLCs can vary. If you explain that the LLC is a sole-member entity which has no employees and no income, they should have no issue adding this without additional fees. You may want to also explain that you will be the only driver. If using a trust, the insurance company may request trust documents, and the Certificate of Trust should be sufficient.

Loans

All of the scenarios I presented involved a vehicle purchase with cash. If you require a loan, it will complicate things. While many lenders will title a home loan in a trust, most vehicle lenders do not like this. I encourage my clients to purchase a tier of vehicle that can be paid in cash.

This may result in a used vehicle from an individual. In my opinion, the privacy benefits when purchasing with cash outweigh the luxuries of a fancy car with a loan.

Choosing a Vehicle

One goal of vehicle privacy is to not stand out. Purchasing a bright pink Cadillac or brand-new Lamborghini will generate a lot of attention. People will want to know more about you. I encourage you to always consider vehicles that will blend into the community where you live and avoid anything that is not common. At the time of this writing, the following were the most common new and used vehicles, spanning sedans, SUVs, and trucks.

Nissan Rogue	Toyota Rav4	Toyota Corolla
Honda Accord	Toyota Camry	Dodge Ram
Honda Civic	Honda CR-V	Ford F-Series

The color choice is also important. Red, green and blue tend to be a bit more unique than common colors such as grey, black, and white. Imagine that you drive a grey Honda Accord. You unfortunately find yourself involved in an unjustified and aggressive road-rage situation that you try to avoid. You escape, and the offender finds himself stopped by the police. He blames you for his erratic behavior and demands the police identify you. He can only provide that you have a grey car and it was a foreign model. That description will likely match at least 20% of the vehicles traveling on the highway at any given time. The same cannot be said about a powder blue Nissan Cube.

This is all likely common sense to many readers. What is often ignored are the various features that make a car stick out to a casual observer. Those custom chrome rims and low-profile tires are not standard stock options and provide an opportunity for a very detailed description in order to identify you quicker. The raised spoiler and upgraded blue headlights make you unique from anyone else on the road. Please consider the most boring and common stock options. Your desire should be to blend in and remain unnoticed.

Vehicle Markings

If buying a new vehicle, I encourage you to make a few demands before signing any papers. I have found this to be the most opportune time to insist on a few minor details from the sales person, who will likely do just about anything to complete the sale. Most new cars from dealerships possess a custom registration plate frame with the name of the dealer in big bold letters. This is free advertising, and replaces the stock frame originally included with the vehicle. Demand that it be removed and replaced with the bland frame designed for the car. This is fairly minor, and the dealership should be happy to comply.

Next, consider having all brand logos be removed from the exterior of the vehicle. You may receive resistance from this request, but hear me out. When you purchase a new vehicle, the various emblems or make and model identifiers are not mandatory. There are no laws that demand constant announcement of the type of car you purchased. These are nothing more than free advertisement to the car companies. More importantly, they are identifiers to help describe your car to others. The next time you are in a parking lot, imagine each car without the emblems placed at the rear. It would be difficult for the common driver to identify each.

As part of this request, ask that the removed emblems and decals be preserved and given to you. When you sell the vehicle, the next buyer may desire these decals be present on the vehicle as a status symbol. They can always be glued back onto the vehicle. If you plan to execute this strategy, I encourage having the dealer remove the signage. They have the proper equipment to do this easily and without damage. Popping these off with a flathead screwdriver in your driveway will likely produce undesired results. Removing vehicle markings can also backfire on you. If you have a very expensive car, such as a Porsche, with no decals, you may stick out more. You may be described as "the Porsche without the decals". This makes you more unique. I offer this strategy only for the boring vehicles, such as common cars and trucks. For a more exciting approach, you could purchase inaccurate logos from an auto store. Place a Ford logo on the rear of your new Toyota. This is a level of disinformation that will confuse many. While I present this strategy as half-humor and half-intentional, I do not recommend this technique for everyone as it could make your vehicle more unique. I will confess that my truck has absolutely no markings, logos, or dealer advertisement whatsoever.

Vehicle Services

There is a growing industry associated with data collection from vehicle maintenance providers. The next time you have the oil changed at a major vehicle maintenance chain, notice the number of computers involved in your transaction. There will likely be a scanner connected to a computer that will read your vehicle identification number (VIN) and an image of your license plate may be displayed on a screen near your vehicle. This will then populate generic information such as the make, model, and year of your vehicle. It will then query various online databases in order to attempt to populate your name, address, telephone number, and maintenance history, regardless of the alias you provide at the time. The video cameras in the stall which collect your registration plates are connected to a media server that stores the visual depiction of the event. The computer that prints the receipt will receive all collected information and likely include everything in the detailed transaction report. This invasion is at the expense of convenience. As a final blow, all of this will be shared with multiple companies that have no need to know about your desire to change your oil. There is likely someone reading this thinking "No way, that is not how that works". Consider the following which happened to me in 2016.

I drove a secondary utility vehicle which I own to a national oil change service. It was the typical in-and-out in a "Jiffy" style of establishment. I requested a basic oil change. The worker asked for my mileage, which I did not know. Being a difficult privacy enthusiast that resists ever sharing any information, I said that the odometer was broken. The worker entered a random mileage reading and moved on. Less than a month later, I received a notice from my insurance company. Since this was a secondary vehicle with minimal use, I had previously qualified for a reduced insurance rate due to low mileage. The data from the oil change visit was sold to the insurance provider, and they determined that the mileage of the vehicle was greater than expected and the rate was to be increased. While this increase is justified based on the coverage purchased and the inaccurate reading, this proves that these records do not stay within the systems at the repair shops. This is why I only patronize the local independent repair shops, and not any national chains. I tend to get better service while I control my privacy.

Tolls

Some readers can likely remember the days of throwing coins into a toll basket and waiting for the green light acknowledging that you met the toll requirements. I miss these days. Today, it is extremely rare to find a toll road that accepts cash. Instead, the use of various digital transmitters has replaced the necessity to always have coins in the vehicle. These devices, commonly called E-Z Pass, FasTrak, I-Pass, and other clever names, have been great for decreasing congestion and simplifying payment for toll roads. However, they have also taken quite a toll on our privacy. Each device is associated with an individual and vehicle, and all travel transactions are logged permanently. Those of us who possess one of these devices in our vehicle are volunteering non-stop tracking as we lawfully travel on various highways. If you do not want to participate any longer, you have the options of either ceasing use of the devices or obtaining them anonymously.

First, I should discuss the idea of avoiding tolls. In extremely populated cities such as Los Angeles, one can simply stop using the express lanes. This will cause a delay in your commute and may not be appropriate for you. In other areas, such as the outskirts of Chicago, it may not be this easy. The only main roads which will get you to your destination require a toll. In areas that require the use of toll bridges, you may not have an option but to pay electronically. Most areas which have mandatory electronic tolls offer an option to pay online after use. However, this is quite a burden with continuous use. Therefore, for those of you that must participate in the electronic toll system, I offer the following tips for obtaining an anonymous toll transmitter.

Some major cities have systems in place for prepaid toll transmitters. I was pleasantly surprised to find that the Golden Gate Bridge has a web page titled "I Want To Remain Anonymous" at http://goldengate.org/tolls/iwanttoremainanonymous.php. It provides great detail about

how to anonymously purchase a FasTrak device at select stores using cash, and the hours of operation of the office that allows toll funding in cash without any identification. While I do not expect this trend to spread across the world, it is refreshing to see the effort. I suggest contacting your appropriate toll entity and ask if they have an option for "private registration" of a toll transmitter. You will likely receive resistance with this unusual request, but it should be attempted. If (when) that fails, consider the next option.

Most states offer toll passes to businesses which may have multiple vehicles in a fleet. If you chose to register your vehicle to an LLC, you can also register your toll pass to the same LLC. If you did not register your vehicle in an LLC, you can still use the LLC to register the toll pass, but you will lose the privacy protection if the vehicle is registered in your name. If you do not have a FEIN from the IRS, simply write "pending" if requested. Everything else can be the publicly available information associated with your LLC. The payment option can be a Privacy.com masked debit card number. When submitting these applications electronically, a signature is usually not required. Ultimately, the states just want to be paid. As long as you fund the account, pay your tolls, and provide no reason for them to hunt you down, you should have no issues assigning your toll pass to an LLC.

Is this really a concern? Some readers of the first edition told me I was being overly paranoid, as toll readers only transmit minimal information when activated at necessary times. Many do not consider that the unique identifiers transmitted from the device are associated with a real person within the database of that system. I counter their argument with the following situation which earned my client some unwanted attention.

"Jill" had purchased her vehicle in the name of a trust, but continued using her toll pass sensor which was previously registered in her true name. One day, she was contacted at her place of employment by two uniformed police officers. They were investigating a fatality accident in which they believed she may had witnessed. She was unaware of any such incident, but she confirmed that she was driving in that area at the time. The officers thanked her for her time and asked her to call if she remembered anything differently. Before they left, she questioned as to why they had contacted her specifically. One officer disclosed that the toll pass reader near the scene of the accident displayed a log which identified her vehicle as being present at the time of the crash. The toll pass system provided her name, home address, and vehicle details. While at her home, a roommate disclosed her place of employment to the officers. The pressure was now on Jill to explain to her co-workers that she was not in trouble.

As a former officer, I respect the investigation tool that toll pass histories provides during serious incidents. As a privacy enthusiast, I do not want police officers contacting me at my place of employment in front of suspicious co-workers. If I did not witness an incident, I do not want to be identified or contacted at all. My client is probably now documented within

the investigation in which she had no connection. This is why I apply the following policies toward my own usage of toll passes, and encourage others to replicate.

- I try to avoid areas which require an electronic toll pass.
- If unavoidable, I use cash at booths present at entry and exit.
- If required, I purchase an electronic pass in the name of an LLC.
- If purchased, I apply payments from a masked payment source.
- When not in use, I keep the device protected in a Faraday bag.

There is no law which states you must have your toll pass permanently on display, ready to be queried as you drive through various roads. You must only have it present while traveling on a tollway which requires an electronic sensor. Once you leave the tollway, it is possible that additional readers collect device information, even though it is not required for a toll. I believe that any device which transmits data about you or your vehicle should be shielded within a Faraday bag when not in use.

Private License Plate Readers

Years ago, only government entities established license plate readers across major cities in order to investigate serious crimes. After a robbery, detectives could view the logs and determine any vehicles of interest near the crime scene. Today, many private companies are building their own internal networks of license plate location databases. Consider the money McDonald's is spending in order to eventually track all drive-through customers.

In March of 2019, McDonald's acquired a start-up called Dynamic Yield for $300 million. This company specializes in "decision logic" in order to make food and add-on suggestions to drive-through customers who are in line. Drivers would see tailored options on digital menus, based on factors including the time of day and their previous selections. This will allow McDonald's to track your orders, date and time of purchase, vehicle, occupants, and form of payment. Tie that all together, and they will control a very detailed dossier of your dining activities.

When this happens, do you want to be in that system? This is yet another reason why we should always pay in cash and possess vehicle registration which is not publicly associated with our name. In an upcoming chapter, I will expand on the avoidance of private vehicle plate readers within your own neighborhood.

Vehicle Privacy

Your vehicles should reveal as little personal information about you as possible through its appearance. Any personal information that is displayed on your car could be a vector for social engineering and should be avoided. You should also be careful about the personal information that is stored inside your vehicle. I hope the following suggestions will encourage you to revisit the privacy and security of your vehicle's interior and exterior.

The items located inside your vehicle can reveal a lot about you. The discarded receipts, shopping bags, coffee cups, and other debris can reveal information about who you are and your pattern of life. Most of this information can be captured from the exterior of the vehicle. Do you shop at high-end retail stores? This may encourage burglary and theft from you. Do you enjoy a certain, unique coffee shop each day? This indicates a physical pattern of behavior that could be used to execute an attack. Is an electric bill or Amazon package, with your name and address clearly visible, on the front seat? This reveals the location where you will likely be sleeping tonight. Items like these can reveal where you live, where you work, and the things you like to do. Keep this information out of your car or hidden from view.

Documents in your car present an additional concern. First, many of these papers, such as your vehicle registration and insurance documentation, often contain sensitive information in the form of your full name or home address. All of this is information you would not want accessed, lost, or stolen. However, you are required by law to have this information in your car during operation, and it must be reasonably accessible. Complicating the matter, you sometimes must allow others to have access to your car. This can include mechanics, detailers, valets, and others. These people may (or may not) be trustworthy, and would have full access to this information.

The concern is the balance of keeping these documents available and accessible while still protecting them from the curious. If your car has a locking glove box it may suffice to protect these documents, as long as you have a valet key (a key that operates only the doors and ignition but not the trunk or glove box) and remember to use it at all times the vehicle is out of your control. If you are exceptionally patient and dedicated to security, you could take these documents with you when you leave the car, but the risk of forgetting them is high and could have legal consequences. Personally, I carry the minimal amount of required information, including an insurance card and vehicle registration (scanned and reduced in size) in my slim "Driving" wallet. This is the wallet which only contains my true identification, which would be required during a traffic stop. There are no personal documents within my vehicle at any time.

Auto Supply Store Profiles

Have you ever stopped by an AutoZone, or any other auto parts place, and had them help diagnose a "Check Engine Light"? This free courtesy is a smart business move. Their portable machines connect to your vehicle through its OBD2 port, extract various vehicle readings, populate this data into their network, and the cashier can recommend the most appropriate part for your vehicle. You may then pay with a credit card in your name and walk out without much thought about the privacy implications. I know I have in the past. If this describes an encounter you have had at these types of places, they now have a record of the following details.

Your Full Name
Credit Card Information
Vehicle Year
Vehicle Make
Vehicle Model
Vehicle Identification Number (VIN)
Controller ID Number
Trouble Codes
Vehicle Diagnostics
Store Location
Vehicle Parts Purchased
Recommended Purchases

Many may find my paranoia about this behavior unjustified. However, I offer an additional piece of ammunition for my concern. In 2019, I downloaded a "Vehicle Owners" database from a website which sells breaches, leaks, and marketing data. It contained millions of records identifying vehicle owners by name, city, make, model, and VIN. I searched my name and received the following result, modified for my own privacy.

Bazzell, Michael, 2007 Ford Explorer, VIN: REDACTED, Phoenix, AZ

I have never lived in Phoenix. However, in 2015, I stopped at an auto parts store during a road trip full of live training engagements and requested a scan of my vehicle due to a warning light on my dashboard. The store identified the issue and sold me a new sensor to replace the broken part. I likely paid with my real credit card since I was not near my home. While I cannot absolutely confirm this data was provided from the auto parts store, my suspicions are strong. Now, imagine that you applied the tactics from this chapter in order to possess a fairly anonymous vehicle. You would likely be upset if the details were associated with your name and shared publicly. Therefore, we should never attach our true names to vehicles during any type of service or scans. What if you already shared your information with these types of stores? I offer the following advice, based on my own experiences.

AutoZone: Contact a clerk within a store. Ask them to retrieve your customer record within their system. While they should demand ID to prove your honest intentions, most never check and allow anyone to access any profile. The clerk cannot delete your profile and corporate headquarters refuses to acknowledge any similar requests. Ask the clerk to update your profile

with your new vehicle and contact information (have this ready). If necessary, state you are a vehicle enthusiast and you really want your profile to be accurate. Ask the clerk to overwrite the vehicle information, email address, telephone number, and any other details which appear accurate. If willing, ask the clerk to add your home address, and choose a nearby hotel.

Pep Boys: This is similar to AutoZone, but with a couple of differences. In my experience, they do not store a physical address or history of vehicle scans. However, they do store the make and model of your vehicle if you have provided it during shopping or checkout. This can be overwritten by the clerk with any alias vehicle details.

NAPA AutoCare Center: This store was unique in that they could not search vehicle information by name. Only the VIN could be used. This presents a dilemma. We do not want to provide accurate information, such as a VIN, which could be added to records during the query if the system does not already know this information. In my trial, I provided my true VIN without supplying my real name. The correct vehicle year, make, and model populated, but did not include any personal details. The clerk asked if I wanted to add my name, which I declined. I suspect existing details could be overwritten.

O'Reilly Auto Parts: Profiles at this store are unique from the previous three. It was the only store which could delete each field of a profile. Empty fields were allowed. Once this change is saved, the clerk was no longer able to access any data after searching my name or vehicle.

Advanced Auto Parts: This was similar to O'Reilly's, but with one hiccup. The system would not accept an empty field as a replacement for a previous piece of data. However, placing any text, such as "Removed" was allowed. After applying my requested changes, the clerk was not able to retrieve my customer details.

If any stores possess no record about you or your vehicle, then I typically do not recommend creating anything fictitious. However, this does provide a decent disinformation opportunity, so be sure to remember this tactic while reading Chapter Fourteen. In my experience, none of these services will delete your profile. Populating inaccurate details appears to be the only option.

Vehicle Tracking

As the technology inside vehicles advances, so do the privacy concerns. Most modern vehicles have the ability to track numerous aspects of our usage such as location, speed, braking, and overall driving habits. In general, more expensive vehicles such as those manufactured by Tesla will possess more privacy intrusions than lesser-priced vehicles such as base model work trucks. However, every modern vehicle possesses a "black box" known as an Event Data Recorder (EDR). The data gathered by these units is commonly acquired after a traffic crash

which has resulted in serious injury or death. It usually identifies the driving details leading to the incident. For our purposes, I will not try to evade the capturing of any sensitive data. Instead, I want to focus on the prevention of data being remotely shared with any third parties. The first consideration is the type of vehicle which you are purchasing. Do your homework, but also ask the following questions to the sales person.

- Does this vehicle possess a cellular modem? If the car you want has its own internet connection, there is little you can do to prevent data from being sent about your usage. It is impossible to buy a Tesla without a constant internet connection. I will never consider a vehicle which continuously sends data about me to the manufacturer. If a vehicle has OnStar, then it has an internet connection.
- Does this vehicle require a mobile device in order to apply systems updates? This is a good indicator that an internal cellular connection is not included, but can present new concerns. Many Toyota vehicles refuse to allow use of the radio until a phone is connected in order to apply updates. It will also send data out through this cellular connection without your consent. I never connect a mobile device with internet access to any vehicle. When you do, data will be transmitted and stored indefinitely.
- Does this vehicle have an embedded GPS Unit? Is there a service which allows navigation with real-time traffic notifications? If the answer to either of these is "yes", then you may possess a vulnerability. Most vehicles have GPS built into the infotainment system today. You should determine whether a premium service allows data from the vehicle to be sent to the manufacturer. The answer will almost always be "yes". You will likely notice that lower trim packages do not offer a navigation option. This is the desired scenario for me.

Next, avoid any mobile applications created by the manufacturer of the vehicle in order to enhance your experience. Ford has FordPass, GMC offers myGMC, and Chevrolet encourages you to download myChevrolet. While these apps offer great conveniences and entertainment features, they also disrespect your privacy. Let's take a quick look at Nissan, but we could replicate the following intrusions within practically any vehicle mobile application.

Nissan owners have an option to download the NissanConnect app to their smartphones. It allows you to find your parked your car, remotely start the vehicle, be notified about upcoming maintenance, or receive a notification of a collision. In order for this to work, a paid service associates your vehicle with your mobile device. The vehicle possesses an ability to connect to the internet, likely through a cellular modem, and the service allows it to maintain a connection to Nissan. This convenience presents two issues.

First, there is a huge security concern. If your phone is lost or stolen, there is an avenue to breach your vehicle. Even if your device is safely in your possession, car hackers have proven many times that vehicles are prone to unauthorized access. Next, there are several privacy

implications. The privacy policy for NissanConnect states very clearly that they can share any data about you and your vehicle with other companies. In 2020, Nissan updated their policy with the following entry, without any consent from users.

"If you are a registered Nissan owner and NissanConnect Services subscriber, this update allows Nissan to share information such as your vehicle's mileage and vehicle location with third parties."

If you have already downloaded a mobile application provided by your vehicle manufacturer, registered an account through their service, and associated your vehicle to the account, you should consider wiping your tracks. This should be done in a very specific order.

- Attempt to remove any accounts within the vehicle's infotainment unit. You might see a profile in the settings menu.
- Conduct a hard reset of the infotainment unit, which should return the configuration to the default which was present during purchase. You may need to find instructions within your vehicle manual or online.
- Disconnect the vehicle battery for at least one minute, which may remove leftover unwanted data.
- Through the app on your mobile device, attempt to remove any association to your vehicle. Afterward, uninstall the app from the device.
- Log in to the account through the designated web page within a web browser. If the vehicle is still present, attempt to remove the association.
- Attempt to delete the entire account within the account settings menu. If this is not allowed, contact the service and demand removal of all data.

You may think this is all overkill. If you do, I present the story of Mathew Marulla, as originally reported at Krebsonsecurity. Mathew leased a Ford Focus electric vehicle in 2013, but returned the car back to Ford at the end of his lease in 2016. In 2020, he received an email from Ford stating that the clock in his car was set incorrectly. Marulla's credentials from 2016 still worked on the MyFord website, and he was presented with an online dashboard showing the current location of his old vehicle and its mileage statistics. The dashboard also allowed him to remotely start the vehicle, as well as lock and unlock its doors. He provided the following statement to Brian Krebs.

"I can track its movements, see where it plugs in," he said. "Now I know where the current owner likely lives, and if I watch it tomorrow, I can probably figure out where he works. I have not been the owner of this vehicle for four years".

If you plan to buy a used car, you should check whether it is possible to reset the previous owner's control and information before purchase. You may also consider demanding that the dealership completes this task. My vehicle tracking rules are quite simple.

- Never purchase a vehicle with an embedded cellular connection. This includes OnStar or any similar competitor. Even when deactivated, the connection still allows remote access and submits data back to the provider.
- Never purchase a vehicle with embedded navigation including real-time traffic information. This indicates an active connection to the manufacturer.
- Never connect a mobile device with internet access to the infotainment unit of the vehicle. This allows data to be sent to the manufacturer.

When playing by these rules, you will encounter minor inconveniences. I received the following complaints from my clients, which include my recommended solutions.

- **Navigation**: Seeing your navigation map on the in-car display is nice. It might also share internet with your vehicle's reporting system. My only solution to this is to rely on your mobile device's navigation on the device's screen. If necessary, mount the device above your dash using a suction mount.
- **Music**: One benefit of connecting a mobile device to the vehicle is the ability to stream music stored on the device or from online streams. Most modern vehicles possess a USB port which accepts flash drives full of MP3 files. My own vehicle allows a 256GB flash drive containing hundreds of albums worth of music. I play the files through the main infotainment dashboard.
- **Podcasts**: Streaming a podcast from your mobile device through your vehicle's Bluetooth is very convenient, but risky. You could load MP3 audio files of podcasts onto the USB drive mentioned previously, but that can be daunting. Instead, I recommend simply connecting your mobile device to the audio auxiliary (AUX) port. No data is transmitted through this 3.55mm audio input.
- **Hands-Free Calling and Texting**: I understand the desire to connect your phone to the vehicle in order to make calls while driving. Many state laws allow this but have ruled touching the phone as illegal. My only solution here is to avoid calls and texts while driving. I know this is unpopular, but we survived without it for decades.

Insurance Apps

I avoid installation of any applications created by my vehicle insurance provider. While you may receive a slight discount in exchange for activating their app, all benefits to you stop there. The insurance companies have much more to gain from your willingness to share personal data with them. The biggest concern is the potential abuse of location information. Many vehicle insurance applications quietly run in the background at all times. They use your constant location to determine speed of travel and other driving habits. This data can then be used to determine your premiums. It can also be used to identify the location of your home, workplace, lovers, and entertainment. Did you park outside a pub for three hours and then race home? That would be documented forever. A dishonest I.T. employee at the insurance company could gain access to this data, and a court order could demand legal release of all collected details. I will not take this risk.

Summary

I realize this can be overwhelming. I have always resisted providing this level of detail in my books in order to prevent confusion or provide too many options. We do not need to overcomplicate the issue. Overall, there are three vehicle purchase choices which will lead you to the appropriate answers:

- Do you own a vehicle titled in your name? Transfer to a trust, with you as the trustee, within your state of residence or domicile. Ensure that the Trustee name is not present on the owner line of the application and that only the trust name is displayed as the owner of the vehicle. If this is not possible in your state, consider the following options.
- Are you buying a new vehicle? Title into a trust with someone else as the trustee within your state of residence or domicile. Ensure that the Trustee name is not present on the owner line of the application and that only the trust name is displayed as the owner of the vehicle. If this is not possible in your state, consider the next option.
- Does your state enforce publicly displaying the trustee name on the title and registration? Consider the LLC route. Seek approval from your insurance provider and investigate any state requirements for foreign business registration and taxes. This route may be more expensive, but may be your only option in a few states.

In any scenario, make an effort to exclude any name and home address from the registration. This step will prevent multiple private companies from collecting, recording, sharing, selling, and accidentally leaking your personal information to the masses.

Chapter Seven

Private Temporary Housing

I have not booked a hotel room under my true name since 2013. This may sound ridiculous and paranoid, but since you are this far in the book, I accept this risk. In late 2012, I was scheduled to present a keynote at a large conference in Florida. This was a very public event, and the roster of presenters was available on the conference website. I was contacted by a person asking if I would be willing to meet her for dinner the night before my session. She wanted to "pick my brain" about some issues she was having, and knew I would be in town. A quick search of her email address revealed dozens of messages sent to my public email address listed on my website. These messages were very concerning, and included allegations of alien probes, government chips in her head, and an overall theme of mental instability.

I politely declined to meet, citing a late flight and early morning. She responded notifying me that the last flight into the local airport from St. Louis arrived at 6:15 pm and that we would have plenty of time. I again declined, and did not think much more of it. I arrived at my hotel at 7:00 pm, checked in, and walked to my room. A woman was following me, so I took a detour into a stairwell. She followed and sternly stated that she needed to talk with me right away. I returned to the lobby, and we had a very brief conversation. I clearly explained that her actions were inappropriate, and she agreed to leave. I did not sleep well that night.

This may sound like minimal risk and you may think I am the jerk for declining to help her. For a moment, replace the players. Pretend my role is played by a successful woman in the entertainment industry, and the original woman is now a male fan that has sent threatening letters. It may not seem so crazy now. This scenario happens every day. Many of my clients find themselves constantly harassed by people that just want to be closer to them. This includes celebrities, business leaders, and domestic violence victims. You do not need to be famous to have a violent person in your life. Therefore, we must have plans for anonymous housing, even if temporary.

This chapter is a transition in order to prepare you for the ability to purchase your next home anonymously. While you are hunting for the perfect new home, you will need temporary housing. This chapter will define temporary housing as short-term options such as hotels and longer-term solutions such as rental homes. Let's start with the easier of the two, hotels.

Obtaining a hotel reservation is very difficult without a credit card. Some hotel operators will reserve the room without a guarantee that it will be available. Some will refuse the reservation without a valid card number. Lately, many hotels apply the entire charge for the visit at the moment of the reservation. When you arrive, you must provide the card at the front desk to be swiped. This collects the data about the cardholder and attaches it to the sale. There are two main reasons for using an alias while at hotels.

When you stay at a hotel, there is a lot of information that the business can analyze about you and your stay. The amount you paid, the length of your stay, any amenities you purchased, and the distance you traveled from home will be stored in your profile. This will all be used to target you for future visits. Worse, it will be shared with other hotels in the chain that can benefit from the data. Even far worse, all details are leaked publicly though a data breach, similar to the Marriott breach of 2018.

A more serious concern is for a person's safety. If you are the victim of a stalker or targeted by someone crazy in your life, it is not difficult for them to find out the hotel where you are staying. The easiest way would be to contact every hotel in the area where you will be traveling. The following conversations with a hotel operator will usually divulge your chosen hotel:

"Hello, I made a reservation there a while back and I need to add an additional day to my stay. I may have put the reservation under my wife's name, Mary Smith. If not, it could be under my name, Michael Smith. I'm afraid I do not have the reservation number; can you find the reservation without it? It is for next week."

The operator will either be unable to locate your reservation or confirm that an extra day was added. The first call which receives the confirmation will identify where you are staying. A simpler approach may be the following:

"Can I leave a message for Michael Bazzell? He is staying there now."

The response will either be, "We do not have a guest here under that name", or, "Yes, go ahead and I will leave the message at the front desk for him".

A more high-tech approach could be conducted through the hotel's wireless internet. Many hotels require you to log in to the wireless internet before you use it. This usually requests your last name and room number as verification that you are a valid guest. Some amateur programming can create a script that will attempt to log in with your last name and each room number of the hotel until the attempt is successful. This not only identifies the hotel where you are staying at, but exposes your room number. This can be a huge security concern.

You can use an alias name to create your hotel reservation. Since you are not committing any type of financial fraud, I believe this is legal. You will be providing a legitimate source of payment and will pay all charges in relation to the stay. There are two main attacks for this, as outlined in the following pages. The first requires no identification, but carries a bit of risk.

Many hotel chains offer prepaid reservations and digital check-in. I have had the most luck with Hilton properties. I recently needed to travel domestically to an airport hotel, and then internationally for a few days. I wanted to stay off radar and test a new strategy on which I had been working. I have had the best success with the following routine.

- Create a new rewards account with a large hotel chain, preferably Hilton or Marriott. Use any alias name, and any physical address, such as another hotel. The longer this account can "age", the better your chances of success.
- While logged in, search the hotel website for a hotel near the desired location. Watch for notifications about "Non-Refundable". This is actually the desired option.
- Attempt to identify hotels that offer "Digital Keys". This allows you to use a mobile device to unlock the door to your room, often bypassing the front desk.
- Book your room, pay with a prepaid credit card, secured credit card, or Privacy.com debit card. All of these options will be explained later. Use the same alias details connected to your alias rewards account.
- The day before your stay, pre-check into your reservation and choose a desired room with the hotel's interactive online reservation system. Most Hilton properties allow this.
- If you selected a hotel with a digital key option, you should be able to unlock the door with your mobile device. This requires the hotel app to be installed, so I maintain an old Android device solely for this purpose. You can connect to the hotel Wi-Fi through this device and unlock the door from the app.

As always, there are caveats for this to work. Generally, the first time you use this feature, the hotel will ask you to check-in with the front desk. They may want to see identification and the credit card used during the registration. The Hilton website makes this clear with the following disclaimer.

"For Digital Keys: Most new digital key users will need to stop at the front desk upon arrival to activate their digital key. Must have iPhone 4s or newer running iOS 8 and higher or an Android phone running version 4.3 or higher with Bluetooth Low Energy enabled phones."

I have used this technique on numerous occasions. The resistance from the employees at the front desk has varied. In three recent attempts, each with new rewards accounts, I was able to gain entry to my room without displaying any type of identification. All three required me to

check-in with the front desk before my phone could be allowed to unlock my room. In all three, I opened the communication with the following dialogue.

"Hi, I have a room prepaid with digital key check-in, but my app says I have to check with you to enable it. Can you help?"

In each scenario, the hotel employee requested photo identification and the credit card used. My response each time was the following.

"I didn't bring my wallet in with me, and my ride has already left. I assumed since I could use my phone to bypass the front desk you would not need that. In fact, your site says that would be the case. If you would like, I can show you my app, confirmation, and receipt of purchase to justify the stay."

This verbiage has always de-escalated any resistance. You may encounter a difficult employee that stands his or her ground and demands identification. When this happens, I have found a polite request to bring my ID before check-out works. I also always have the Hilton website discussing the ease of digital keys pulled up on my mobile device web browser, which I can display to the hotel employee in my defense. It can currently be found on their website at https://hiltonhonors3.hilton.com/en/hhonors-mobile-app/digital-key.html.

I have also tried prepaid options without digital keys, and had no issues at check-in. When I did not have the option for digital keys on the website, my room card was waiting for me at the front desk. Since the rooms were prepaid, I was usually not asked for any ID or credit card. The vital piece for all of this to work is to book rooms which are completely prepaid, non-refundable, with successfully charged fees through your payment method. Once the hotel has received their payment, identification and credit card requirements are more lenient. If you are pushed to provide the physical credit card used during purchase, blame your employer. I have found stating, "My work paid for the room with a corporate credit card. I WISH they trusted me with having a card, but you know how THAT goes". I have yet to be challenged on this.

I will end with a warning. This could fail. You may be denied a room. I find this to be highly unlikely, but it could happen. Also, if you need to cancel a reservation, you will not receive a refund. I only provide this information for those that need it. Domestic violence victims, stalking victims, and those under a temporary spotlight may find this useful. I consider many options when I assist someone with disappearing completely.

In early 2020, I attempted these techniques at an affordable hotel in an urban area. I could sense suspicion from the staff toward every customer. This hotel was in a high-crime area, and the employees seemed on high-alert. I dished out every excuse in the book as to why my client,

a domestic violence victim who fled her tech-savvy abuser, had no government identification in the name matching the registration. They were not budging. I was told that she would not receive a room without ID and a physical credit card in that name. I advised I would make a call and come back in a few minutes. A quick Google search identified the hotel owner's name and Truepeoplesearch.com disclosed his home address and landline telephone number. Out of desperation, I told the clerk, "I just spoke with (owner name) and he asked you to call him at home at (home number) if there were any problems. He is a friend and is helping me relocate an abused woman". I sweated a bit from my ruse until she said, "That's fine, I am not calling him this late". That night, I began questioning this line of work.

The next tactic provides more assurance that you will have a smooth interaction with the front desk, and check in under an alias with no resistance. This requires a credit card in an alias name, which is explained in the following anonymous payments chapter. These are fairly easy to obtain and are completely legal. The difficult part of this plan is identification in the alias name. Many people will not be comfortable with the following methods, but my clients in fear for their lives have no issue.

First, create a new rewards account with a large hotel chain, preferably Hilton or Marriott, as previously mentioned. Use any alias name, and any physical address, such as another hotel. This can be created the day of the booking. Upon arrival at the hotel, hand your alias credit card (explained soon) to the receptionist. You will likely be asked for identification. In my experience, stating that your wallet was stolen and you only have the credit card because you keep it in the car is sufficient if you really "sell" it. Your success will vary widely. I always recommend persistently denying that you have ID if you have nothing with your alias name on it. Possessing your rewards card in your alias name is often enough to pacify the request. Very few hotels will turn down a loyal paying rewards member with a credit card in hand. I find that being polite and understanding always works better than acting agitated.

If this does not work, have a travel partner show identification to meet the requirement. This information will most likely not be added to the reservation, and cannot be queried. In 2017, I was checking into the Mandalay Bay under an alias name before the BlackHat conference, where I was teaching a 2-day privacy crash course. I provided my alias name and credit card, but the card was declined. I had not used that card for many months, and the provider blocked the charge as suspicious. Fortunately, a colleague was with me and stepped in with his credit card and ID to meet the requirement. He was not staying in the room, his details were not attached to my stay, he was not tremendously exposed, but he would get billed if I trashed the room (I did not). This is not the best option, but will suffice if desperate.

I prefer a third option. I possess alias identification at all times. Hear me out before you believe I am breaking the law. I would never condone obtaining a real or fraudulent government identification card in your alias name. Not only is that illegal, but completely unnecessary.

Instead, I create my own "club", which I am the founder (as my alias name of course). For example, you may be very interested in rock climbing. You could start your own organization titled "The Greater Houston Rock Climbing Gym". Maybe you have some steps on your back porch that you use to "climb". Your definition of climbing might be different than others. Now, you may choose to create an identification card for the members of your backyard gym. This could be completed in Microsoft Word and may include a photo of you. Your local print shop will happily print this on a nice paper stock and laminate it for you. The following should work well at the check-in of your hotel.

"I'm sorry, I left my license at the gym, can I show you my gym membership card until I go back to get it?"

I have also found employer identification to satisfy a demand for ID at a hotel. Assume I possess an LLC titled "The Workplace LLC". I can create an employee identification card containing my photo, alias name, and company logo. I can then place this laminated card into a lanyard around my neck during check-in. The moment I am asked for identification, I do a quick pat-check for a wallet on my back pants pockets and then instinctively grab my lanyard. I pull it toward the employee and allow them to verify that the name matches the credit card. This has never failed me. For added comfort, I add the line "For novelty purposes only, this is not a true ID, and is not to be used for any official identification" on the back (which is never seen unless inspected closely).

There has always been great skepticism about the legality of using an alias. I firmly stand by my views of when it is legal and illegal to use an alias throughout everyday encounters. I offer my opinion.

- **LEGAL:** Non-government identification in an alias name can be legal. There should be absolutely no mention of any government entity. There should be no mention or reference to any real businesses. It should not identify you as an employee of a legitimate company which you do not own.
- **NON-LEGAL:** Any false identification that displays the words city, county, state, government, police, license, driver, court, agent, et cetera is a crime. Any reference to ANY government agency is also illegal. Any resemblance to a real driver's license will get you arrested.
- Never use an alias when identifying yourself to a government official.
- Never use another person's SSN or known real name and DOB combination.
- Never attempt to obtain any credit under an alias name.

Overall, I believe it is legal to provide an alias name to a privately-owned hotel. Do you think famous celebrities stay under their real names? I can verify from personal experience they do not. Why shouldn't you have the same luxury? After the Marriott breach in 2018, people asked

if I was concerned. I was concerned for other people, but not myself. My true name does not exist within it. My stay history and payment methods are all in various alias names that are not associated with me. I anticipate more hotel breaches will happen, and my true details will not be exposed.

If you are still uncomfortable possessing an alias identification card with alias credit card, there are other options. I have had great success using services such as Airbnb for temporary stays. In fact, it can be easier than traditional lodging. I have arranged lodging through this service for myself and clients. I simply needed to create an account in an alias name, provide some standard details such as an alias email address and telephone number, and select the property where I needed to stay. I always try to find a location that appears to be a secondary home of the provider or an apartment detached from the renter's residence. Once you have provided acceptable payment through the service, such as an anonymous payment source that is explained later, the individual provider is happy to hand you the keys. They rarely ask to see any type of identification or proof of credit card. Often, a code to a digital lock is given and you never have any contact with the host. This situation can be much less stressful than convincing a hotel clerk you are someone else.

I have had several clients recently report that services such as Airbnb were becoming stricter toward new accounts. Rental attempts using a new account, prepaid card, and alias names were being rejected because of new fraud prevention strategies. I no longer book directly through Airbnb. Instead, I contact home-owners directly, outside of the application. This is legal to do, but the Airbnb members may be violating policy by conducting business outside of the app. I often use the Airbnb website in order to identify the place where I want to stay. I then conduct a search of the address within various people search websites and identify the owner. Finally, I contact them directly through a publicly listed email address and offer cash for the stay. Some avoid this for liability reasons, but most welcome an opportunity to be paid in cash and avoid the Airbnb fees.

The idea of providing an alias name and anonymous payment method works in most short-term stay situations. Whether a traditional hotel, extended stay alternative, or privately-owned property through an online service, they all simply want to be paid. They also want empty rooms filled in order to meet strict quotas. As long as you ensure that payment is made and that no financial fraud occurs, you should have no issues using an alias. If you need something more long-term, you will need to change your strategy.

In 2020, I began registering most hotel rooms in a business name. This cannot usually be done online, but a call during business hours works well. I explain that I would like to prepay for a block of rooms in the business name and make sure my employees are not charged anything. In this situation, hotel staff are much less scrutinous toward ID and payment options. Your experiences may vary, but this is another tool to possess.

Reward Programs Concerns

Most enjoy a free stay or a complimentary upgrade at a hotel due to loyalty points. However, these come with serious privacy disadvantages. When you use the same loyalty account for all of your stays, you create a permanent record of your travel. You also generate a pattern of your history which could be used to determine future locations. If you always stay at a specific hotel over winter holidays while you visit family, and I can see your past stays on your account, I can assume where to find you at the end of the year. Theoretically, only hotel employees should be able to access these details, and this may not be a huge threat. Unfortunately, data breaches, rogue employees, and social engineering make this information visible to anyone who desires it. The simple solution is to either possess several loyalty accounts or none at all.

I currently have a loyalty card with both Hilton and Marriott in three different aliases. I switch it up while I travel and book my rooms with the lessons explained previously. However, if I am staying at a property where I will be meeting a high-risk client, I use no loyalty account at all. I use a clean alias with no history. These rewards profiles can assist with smooth check-ins, but come at a price. There is always a trail and you cannot delete your account afterward.

In 2017, I possessed the highest tier of rewards for each major hotel provider. I received frequent room upgrades, free cookies and fruit plates, and more free stays than I could use on personal travel. However, I gave it all up. The perks did not justify continuing the tracking of my whereabouts, even if under an alias. It was only a matter of time before the account was somehow associated with my true identity.

This brings up a scenario which I encounter often. A client needs to disappear, is ready to start using an alias during travel, but does not want to give up those hard-earned hotel points. I do my best to convince them that free stays and upgrades are not worth the risk. Some listen, others do not. If necessary, I encourage them to use up all the points with their family at a posh resort and get it out of their system. We can then start over when they return. Others absolutely insist on maintaining their status while using a different name. This is possible, but not advised.

Hotels do not allow you to transfer your points to another person. However, they allow you to update the name on the profile if you experience a name change. This is most common after a marriage (or divorce), but they also allow any type of legal name change. I am not suggesting my clients change their names (more on this later), but I have assisted one client who really wanted to keep the points. He downloaded a name change form from his state, completed all the fields, and submitted it to the hotel chain. The legal paperwork was never processed through any government entity, it was just sent straight to the hotel. They accepted it and updated the name on the account. Again, this still associates you to your alias, and eliminates most of the privacy of using an alias. I do not recommend this technique.

Places to Avoid

If I want privacy, I avoid fancy hotels and resorts. There was once a day when the rich and famous could enter the Ritz Carlton and expect a private and discreet experience. Today, prestigious entities present more privacy invasions than the smaller chain hotels. The following presents several scenarios I have witnessed on behalf of myself and clients.

- In Los Angeles and New York City, paparazzi stage in front of posh hotels hoping to photograph a celebrity. I have walked into a Holiday Inn with a household-name celebrity and no one noticed. I try to avoid places frequented by photographers with no morals.
- At fancy resorts, staff are trained to memorize the names and faces of all guests. They are also instructed to greet guests by name at all times. Loud echoes of "Hello Mr. Bazzell" any time I walk out of my room are not desired.
- Some resorts advise their staff to research guests in order to make small talk. While at a resort in Grand Cayman during a keynote under my real name, a beach concierge with whom I had never met asked me how the weather was in South Dakota. I don't think he knew what a PMB was.
- While at a beach resort in an alias name during a privacy consultation with a wealthy client facing death threats, I was approached by the pool concierge. She stated, "It is great to see you again Mr. (alias)! I can't believe it has been two years since your last visit!" I don't believe that she remembered me. I suspect she was told my name by other staff, researched my past stays in the internal computer network, and then attempted a conversation which would make most people feel special. The only thing she accomplished was to convince me I needed to change up my alias.
- While checking into a resort, the staff demanded to know my flight number for my departing flight. I was using an alias at the hotel but my true name during air travel. I provided a false number, and was immediately told it did not exist. I conducted a quick search and provided the details of a different flight. This sufficed until staff arrived at my room at 7 a.m. to escort me to checkout in order to make my flight. I should have paid more attention to the departure time of my alias flight.

Overall, you are watched, monitored, and tracked more in expensive resorts than any other short-term lodging option. These are all minor issues to most, but could be devastating to someone trying to disappear. This provides numerous opportunities for an adversary to identify your room number by simply following you and listening to employee chatter. I would never consider placing a victim in this situation. I prefer the anonymity of standard hotels where the staff cares very little about your presence.

Rental Homes

You may need to rent a home indefinitely or while you are purchasing a house. The methods for each are identical. When I need to find a rental home for a client, I insist on the following.

- The house or unit must be independently owned. Large apartment companies will demand a hard credit check and valid SSN from the applicant. This is a deal-breaker. Independently-owned buildings possess owners who can make their own decisions without following a policy manual. Cash can also influence a landlord.
- Utilities must be included in the rent. This often leads to higher overall costs, but better privacy. I will not need to convince the power company to accept an alias name without DOB and SSN in order to activate service. We will tackle that later with a home purchase, but included utilities is optimal while renting.

I always start my rental home hunt through traditional advertisement avenues. I avoid Zillow and other online options. These tend to cater to larger rental companies or individuals with numerous properties. These scenarios often lead to meetings with property managers on behalf of the owners and an immediate application including background check and credit pull. Instead, I start with newspapers.

I found my first apartment in the classifieds section of a local newspaper. This may show my age, but that was the only option back then. Today, many modern rental offerings avoid printed distribution, especially when the internet provides a broader reach. In my experience, the perfect landlords are those who still advertise in the papers. I try to seek out those that have only one or two rental units and prefer to place signs in the yard instead of hiring property managers to recruit tenants. A later chapter tells a true story of working with a private landlord in order to hide a client. Until then, I will include a few notes about the process.

Background checks and credit pulls are off limits. Some may believe that these inquiries do not attach the client to the future rental address, but I disagree. Services such as Experian's Tenant Credit Check and others ask for many sensitive details such as the name, DOB, SSN, and previous addresses of the prospective tenant (the client). These details are also demanded from the landlord. Experian will possess full rental histories of previous tenants from this landlord who chose not to protect their privacy. Therefore, Experian already knows the likely address of the rental unit. They can easily associate the client with the address before the credit report is created. This data is then shared with other divisions of this data mining empire, as well as the next inevitable breach.

My ultimate goal is to never reveal the true name of the client to a potential landlord. Once I find a property suitable, I make direct contact with the owner. I explain that my client is a domestic violence victim and is scared to tell anyone where she lives. When I encounter a

landlord who has no empathy for this, I move on. I always offer a cash deposit and first month of rent, as well as the promise of a cash monthly payment in advance. This goes a long way. In dire circumstances, I have offered up to six months cash in advance for the luxury of anonymity. There is no magic to this. You simply need to find the right property owner. Cash is king. It will provide more negotiation power than you might expect. My experiences with a client which are explained later will provide much more detail.

In 2020, I began using my business in order to ease the process of finding short-term rental homes for clients. I established an "anonymous" LLC for this purpose, obtained an EIN, and opened a checking account. I always keep a packet of LLC documentation ready to show a potential landlord. This includes the certificate of organization, confirmation of EIN from the IRS, recent bank statement, and LLC checks. This new method has worked amazingly well, and was created after a conversation with a friend who travels long-term for work at various refineries. I asked him how he handled rental housing, as I know he relies heavily on cash while on the road and can be gone for six month stretches. He advised that he never arranges or pays for rental homes because his employer handles all of the logistics. This changed how I look at rental homes for clients needing three to twelve months of temporary lodging. My first test was in January of 2020 when a client requested assistance leaving an abusive situation.

She located a small home for rent by an independent landlord which included utilities. I asked to see the home and met with the owner. I advised that I owned a small company and needed temporary housing for an employee who was relocating to the area and was having trouble finding a home to purchase. I stated that my business would pay the rent and eagerly provided all of the paperwork mentioned previously (none of which included my name). I encouraged the owner to verify my business details with the IRS and the bank. I also offered a "proof of funds" letter from the bank disclosing the current balance to settle any fears that the owner may have about getting paid. I offered to write a check for the first and last month on the spot and agreed to go to a local branch of the bank, if he desired, in order to verify the check. The owner agreed to rent the home directly to my LLC with very little interest of knowing the employee's name. He was more interested in my line of work. I told him I managed finances for wealthy people and my new employee was in training for a similar position. Technically, this was the truth. I do receive payments from wealthy people for various services, and I would be teaching my client ways to replicate my process for her own benefit.

Since this experience, I now have a better understanding of the overall tactic. Most landlords assume that a business is less likely to stiff them on rent than an individual tenant. They also hope that future rental opportunities may exist from my business. Best of all, I now use these positive experiences whenever an owner wants a reference. I recently witnessed a potential landlord call a previous landlord asking about my LLC as a renter. After their quick conversation, I wrote a check and received keys to the home. Neither of them knew my real name. Much of this technique involves confidence, manners, and respect toward the owner.

Hidden Cameras and Unauthorized Entry

Regardless of whether you are in a hotel, Airbnb, rental home, or any other type of lodging, you should be aware of hidden recording devices and unauthorized access to your living space. In the past two years, I have had two clients who were surreptitiously recorded nude in hotel rooms and extorted for money over the recordings. Due to pending civil litigation, I cannot speak about those specific events. However, I can explain a typical extortion process which has recently impacted hundreds of victims nationwide.

The typical hotel customer provides his or her real name, home address, personal email address, and cellular telephone number during the registration process. By now, you know that this is risky behavior. However, I suspect that over 99% of all hotel guests have no concerns about privacy and willingly hand over these details. This information can be used against you when a rogue employee wants to contact you with threats of releasing sensitive content. Consider the following fictional example, based on true events.

- The night manager of a hotel is a creep and installs a small hidden camera in the bathroom of a few empty rooms. He places the devices behind some folded towels, in a tissue box with a pinhole, or within the shell of a smoke detector.
- The device is battery powered and recording is enabled by motion sensitivity. A micro SD card stores any video recorded.
- You check into this hotel under a real name and email address.
- The night manager assigns you to a room he knows to possess a hidden camera.
- You enter the room and change clothes and shower as normal.
- You check out the next day.
- The manager arrives for his shift and enters the empty room you were assigned. He replaces the SD card and inserts the original in his computer.
- He downloads the videos of you nude.
- He searches the customer log and identifies your name and email address.
- He sends you an email from a private account and includes an excerpt of a video displaying you nude in the shower. He threatens to send a copy to all of your friends and family if you do not pay him money or send self-created nude videos.
- You refuse to respond and he publishes the video to dozens of porn sites. He includes your full name within the description. A Google search of your name reveals these videos.
- He locates you on LinkedIn and identifies the names of your co-workers.
- He sends copies of the videos to people within your employment circles. He spoofs an email address to make the message appear to have been sent by you.
- He repeats the process as often as he receives new videos of new victims.

Does this sound ridiculous and far-fetched? It absolutely happens. Search "hidden camera found in hotel room" within any search engine, video website, or social network and you should be presented with plenty of evidence documenting this popular extortion technique. Using an alias is an important step to thwarting this behavior. It does not prevent the capture from a hidden camera, but it prohibits most of the extortion. If you used an alias name and email, the offender will think that is your real information. If he threatens to post the videos with your name on them, no one will know it is you. If he threatens to send the videos to friends and family, he will find no one connected to your alias name. This is only one level of defense toward this type of behavior.

I encourage all of my clients to conduct a thorough sweep for any hidden cameras within all temporary lodging situations. This includes rental homes, as some landlords have been caught spying on tenants. The procedures for identifying hidden recording devices varies from amateur solutions to expensive gear. I will outline my recommendations, beginning with simple and free methods.

- Visually inspect all areas of each room.
- Look for any inappropriate small holes within objects facing the shower or bed.
- Search common areas such as tissue boxes and clock radios.
- Search behind all towels in the bathroom.
- Look for holes drilled into plastic smoke detectors or walls.
- If your room has one brand of fire alarm devices throughout, but a different brand plugged into an electrical outlet, this is suspicious.
- Turn off all room lights and identify any led lights emitting from devices.
- Always travel with a roll of electrical tape. Cover any suspicious holes or lights.
- Unplug the alarm clock and place it in the closet.
- Inspect all vents for suspicious devices.

If you discover anything which appears to be a hidden camera, choose your next steps carefully. First, personally document your findings with photos and videos. Next, contact the police and file an official report. Allow them to retrieve the device and maintain control of it as evidence. Never complain directly to the hotel staff. This could result in destruction of the device and a cover-up. If you are a high-profile target forced to use your real name upon check-in, immediately request a different room after you are assigned a specific room. If a rogue employee has assigned you to a room with a known hidden device, demanding a new room on a different floor may provide a small layer of protection.

Personally, I always travel with a small amount of gear which assists in quickly identifying suspicious devices. There are a plethora of affordable "hidden camera detectors" online, but I find most of them to be useless. Some have reported that viewing the cell phone camera

through the front-facing screen while the lights are out will reveal covert lenses, but I have found this to be unreliable. I now rely on two pieces of hardware any time I stay in temporary lodging.

The first is a Milwaukee Spot Infrared Imager unit. This device was recommended by my friend and former colleague Tom Gibbons, and was discussed on my podcast with him as a guest (Episode 119-How to Find Hidden Recording Devices). This handheld device displays heat sources. Any small camera will possess some type of power and will generate heat unique from surrounding areas. This unit costs $200-$300, but there are more affordable options on Amazon. I will warn you that you get what you pay for with these. If you care enough to search for this type of privacy invasion often, bring the best equipment.

The next device which is always in my travel bag is an old Android mobile phone which possesses the open-source privacy app **Haven** (https://guardianproject.github.io/haven). Haven is an Android application that leverages on-device sensors to provide monitoring and protection of physical areas. Haven turns any Android phone into a motion, sound, vibration and light detector, watching for unexpected guests and unwanted intruders. Before I explain the usage, let's focus on the installation and device selection.

Fortunately, I possess numerous old discarded Android devices from my government days. These are outdated by today's standards, but will function appropriately for our needs. I have tested Haven on a Samsung Galaxy S4 and various versions of the Motorola Moto G series. First, conduct a hard reset to the device, wiping all data and restoring it to the factory default. You can find details for this specific to your device online. Next, install the Haven app from the Google Play store. If you have a rooted phone with a custom ROM, which is explained later, you can also load this app from the F-Droid open-source app store.

Once Haven is installed, scroll through the welcome screens. Select the "Configure" button and accept the default value for each option. You can tweak these settings later if needed. Optionally, add a telephone number for notifications via Signal. I do not use this feature as I do not care to receive remote notifications or connect this device to my Signal account. Your threat model may demand this level of protection. Exit the settings to the main Haven screen.

Please note that this device will only be used for this single purpose (monitoring a room). It will never possess a SIM card and will only use public Wi-Fi. This is a Google hardware device and privacy is always a concern. It should be turned off when not in use and never be present in your home. Therefore, I accept the privacy violations of Google in order to gain the benefits of this app when needed. Please consider whether you need a device like this in your life before jumping in. I also use this Android device to bypass check-in at hotels which offer the ability to unlock the room door wirelessly from the app.

Once you are at the main Haven screen, which will likely display a view from your front-facing camera, choose the settings icon. If desired, enable Video Monitoring and exit the settings menu. Selecting the "Start Now" option on the main screen enables monitoring. The camera will detect movement, the microphone will detect noise, and the internal sensors will detect movement of the device. Begin monitoring and test the settings. When you make a sound, you should see that indication on the home screen. When you move anything in front of the camera, it should detect this activity. You can safely turn the screen off and your device is now monitoring the room.

In a typical situation, I enable all options whenever I leave my hotel room. I place the device propped-up on the desk, leaning against something, in the room while plugged into a power source for charging. The front camera faces the bulk of the room. When I return, I stop the monitoring application and choose the "View Logs" option. This presents any triggers during my absence. This includes any images and videos collected from the camera, audio recordings from the microphone, and notifications if the device was moved. If housekeeping enters the room, I will see video evidence of this and any associated audio files. This small device will let you know when someone entered your room. Further, it allows you to see and hear their actions. This is a powerful tool.

It could also be considered illegal in some situations. A few states in the U.S. are considered two-party states in regard to audio recording. Both parties (you and the people being recorded by your device) must consent to the recording. If housekeeping or anyone else in the room does not know about the recording, they do not consent. This could place you in a criminal situation and must be considered. Furthermore, some other countries have very strict laws about surreptitious recording of any sort. You do not want to be placed in detention in China for such a violation. I have a solution that works well for me.

When I am staying in a hotel, my Android device with Haven installed is always monitoring while I am away from the room. I carry a small laminated placard which states "DO NOT ENTER, RECORDING IN PROGRESS". I place this on the outside of the entry door. This notifies housekeeping of my desires for no one to enter. It also serves as a deterrent to anyone with malicious intent. It indicates that someone is in the room, and this may not be the best burglary target. Finally, this notifies anyone who may enter that a recording device is present. In most situations, this waives any consent issues.

If you chose to enable remote notifications via the messaging application Signal, you can receive the audio and video from your monitoring before returning. This can be beneficial in case you are notified of a threat which would make you stay away from the room. In extreme situations, this app could make you aware of a physical threat from miles away. Imagine if the app displayed video of an intruder hiding under the bed or hotel staff hiding a camera in the ceiling of your room. Again, these scenarios may sound far-fetched to you. For my celebrity

clients, it is more common than most would think. Haven does not work on iOS, but I am fine with that. I would never want this app on my primary communication device. It works best on old phones which can be left behind in your room without worry about theft. Please become familiar with the app before relying on it in a real scenario.

In closing this chapter, I hope that you now have an interest in protecting yourself while away from home. Each layer presented here has an impact on your privacy. Alias names, eavesdropping identification techniques, and intentional monitoring solutions will keep you safe from both random and targeted attacks. If you are considering an escape from an unsafe situation, please start with the following considerations.

- **Plan well, but secretively**. Only tell trusted people about your plans, and only if they truly need to know. Save enough money for your escape without generating suspicion.
- **Wipe your tracks**. Clear any internet search history on any computers which can be accessed by your adversary. Do not leave with any mobile devices previously used. Change your passwords to your email and delete any communication which might reveal your new location.
- **Collect the essentials.** Make sure you possess enough clothes, medicine, and any other requirements to get you through the first stage of your escape. Store this somewhere private and secure until time to leave.
- **Possess all necessary documentation**. Make sure you have your real ID, passport, birth certificate, and anything else in your name. Plan to never return to your abusive environment and possess all essential documents and paperwork required to prove your identity and access any financial accounts.

International Considerations: Many readers have reported difficulties using alias names while traveling in countries other than America. I have also witnessed resistance from hotel clerks demanding to copy my passport. Many foreign countries have rules which require hotels to retain a copy of official identification from each guest. This can be quite invasive. I do not have a magic solution for every situation, but I provide the following experience I had at a Hilton in London in 2018. Upon arrival at my hotel, I advised the clerk that I wished to check in, but had a question to ask first. I explained that I just arrived in London, and that I left my passport at the airport during customs screening. I further explained that I had received a text message stating that my passport was found and that it would be delivered to the hotel the following day. I asked specifically if the hotel would accept the package and hold it for me. This was a ruse, but it set the scene for my inability to show ID. I offered her my secondary credit card in my alias name (which was used to make the reservation), my Hilton rewards card in my alias name, and my "employee ID" from the company I own, also in my alias name. She happily accepted these items, made a copy of my credit card, issued my room key, and assured me that the staff on duty the following day would deliver my package. I suspect she forgot all about me within an hour, and I never provided a copy of my passport.

Chapter Eight

Private Home Purchase

This entire book has been preparing you for this chapter. I believe the single piece of information which should have the most privacy protection is your home address. This is where you sleep, where your family spends time, and where you are most vulnerable. If someone wants to harm you, it will likely be at your home. If a reporter wants to question you, he or she will stake out at your house. If you take no action to protect these details, you will be on hundreds of people search websites within ninety days after purchase of a new home. You will be a single Google search away from complete exposure.

I mentioned a few scenarios previously where you may want to hide your home address. As I am writing this, there is a Reddit thread asking for the home address of Congresswoman Alexandria Ocasio-Cortez. In the first response, the full details of her apartment are legally presented. Last month, an online gamer was "swatted" by police when a competitor spoofed a call to 911 claiming a home invasion in progress at the gamer's address. Last week, a lottery winner was bombarded by members of the press at his home demanding to know what he would do with his millions, while exposing his address to the world. This week, an "Anti-Vaxxer" contacted me because a person with opposing views encouraged Facebook users to send hate mail and "Molotov cocktails" to her home address. Recently, a stalker was arrested for breaking into Taylor Swift's New York apartment. Next week, will someone have an interest in finding you?

We live in an entitled world where everyone believes they deserve access to everything. If you have received public attention for an unfortunate event, protesters believe they deserve the right to scream at you while you try to sleep. If you are publicly involved in a civil lawsuit, journalists believe they have a right to bother you at home at any time desired. I believe things will get worse, and we should be proactive in protecting our address. Because of this, I never purchase a home in my real name, or in the name of a client. I use trusts, LLCs, and nominees to hide the true identity, and I do this while obeying the law.

This chapter will be intense at times, and I do not expect every reader to apply all tactics. I present several options as I go, and anything you do to protect your information helps. I also discuss a few of my failures, which are often the best education. I ask that you take a moment and question your own level of threat. Is it at all possible that an adversary may try to find you? Is there any scenario where having a public home address could backfire on you? If either

answer is yes, I hope you consider an anonymous home. We cannot predict the future. Once an undesirable incident unfolds, it is too late to hide. You simply must be proactive.

The first step toward obtaining your private home is to consider the overall location. You may already know the general area where you want to live, but there are privacy implications everywhere you look. If you have flexibility within the exact area you wish to purchase a home, you should consider the following.

County vs City: In populated urban areas, there can be many privacy benefits to living immediately outside of city limits. Cities usually have more requirements for various licenses and permits. Everything from pets to parking requires personal information, and most will be placed within insecure databases. Counties, especially unincorporated areas, often have fewer requirements.

Occupancy Permits: Some cities and counties require occupancy permits that identify every individual that resides in the home. Providing false information to this government entity is likely a crime. Avoiding the mandatory disclosure will bring unwanted attention to your home. A call to the local housing division should expose these requirements.

Government Presence: I also look closely at the overall level of government presence within the community. While numerous free government services may be welcome to those who desire them, they come at a cost to our privacy. I pay close attention to the presence, and therefore demand, of law enforcement. When I see police cars constantly present in a specific neighborhood, it tells me two things. First, this is likely a high-crime area. Second, there is an increased risk of being involved in a traffic stop or police report, which can become public information. I look for quiet areas without the need for much government presence.

Neighborhood Involvement: I always look at the overall level of involvement of the local residents in the neighborhood. When I see a subdivision with an active Facebook page, I become concerned. This is an outlet for people to complain about their neighbors and speak poorly about others behind their backs. When a new person moves into a neighborhood such as this, especially someone who tries to be private, it usually sparks interest and investigation from people that have nothing better to do.

HOA: Homeowner Associations can be very invasive to new residents. I try to avoid them at all costs. Some HOAs require all new owners to submit full details of all occupants and registration information for any vehicles. This is likely improperly stored and eventually shared with the entire neighborhood. Many HOAs possess leaders that abuse the limited authority they believe they have. Some force you to pay annual fees via personal check, and refuse to accept cash. While you may have success providing alias information, the constant scrutiny is unwelcomed by most.

Next, you should consider the method for your home search. Real estate professionals can be very helpful, and I will discuss choosing a proper representative in a moment. However, you will still need internet search resources. I always recommend conducting your own searches for a while before committing to professional help. This will give you a sense of home prices and areas you wish to target. There are some important considerations when using sites such as Zillow and Redfin.

All real estate search sites will push you to create a free account. This will allow you to save searches and receive alerts after registration. However, an account is not required in order to use the services. I encourage people to keep their own notes and never create an account. These sites contain powerful analytics that track users. The information collected about your home preferences, IP address, third-party cookies, and provided details creates a very unique profile, which is valuable to data mining and marketing companies.

Whether you choose to create an account or simply search "anonymously", there are some best practices. Always use an isolated browser which is not connected to any personal accounts. You could install a browser such as Brave, and only use it for home searching. Do not sign in to any other services, especially email accounts and social networks. This isolation will prevent some personal data leakage. If you only wish to possess a single browser, such as Firefox, you can take advantage of Firefox's Multi Account Containers to separate home related traffic. If this concept seems difficult to you, it is much easier to simply possess a secondary browser. Alternatives to Brave include Epic and forks of Firefox such as Pale Moon and Waterfox. If you do not already use the Brave Browser, it is a great option for your home search.

Next, you will likely need a real estate professional during your search. The internet has given us most of the tools we need to find a home, but the viewing, negotiation, and closing processes are still easier with professional help. Since real estate commissions are usually paid by the seller, there is little reason to do this on your own. However, use caution. Many real estate representatives are pushing clients to sign contracts guaranteeing a commission. If you choose a house for sale by owner, you may be required to pay your chosen representative a percentage of the sale price. If the seller does not agree to the commission, you are on the hook. I never commit to real estate help until I have found the right person and the right contract. Many reputable representatives will not require a contract until you are ready to make an offer. This varies by location.

Choosing the right person to aid in your home search is very important. This is not the time to simply hire the last person you met who was showing an open house you visited. Because you will be purchasing the home anonymously, you need experienced help. When I am searching for a real estate professional (not all of them are "agents" or "brokers"), I start with an online query. I search for the styles of homes which interest my client. Next, I make a list

of candidates who are selling these homes. I then read reviews and eliminate anyone that seems to constantly generate negative comments. From there, I contact each via email (the proper address to use is discussed in a moment) with the following message.

"Hello, I am new to the area and looking to purchase a home in the near future. Your online reviews were great, are you accepting new clients? If so, I will be purchasing under the name of a trust. Do you have experience with this? Can you disclose any of your experiences or any nuances with purchasing under a trust in _____ county? Thanks!"

In my experience, this will generate three types of responses. The first will be no response at all. You may seem difficult right away and not worth their time. Good, weed those people out. The second response is a canned message telling you how great they are and asking you to schedule an appointment. This may be acceptable, but only as a last resort. If you emailed enough people, you should see a third type of response. It will be very specific, directly answer your questions, and display confidence in the ability to title a new purchase in the name of a trust. This is the type of person we want. Schedule a couple of house-viewing appointments and see how you feel about the relationship. This person will be heavily involved in your home purchase.

My next test is to identify the person's willingness to assist in my quest. I first ask which title company they recommend, and then follow with, "What are their requirements to title into trust?" If the real estate representative reaches out, finds the answers, and provides the information to you in a timely manner, I place them ahead of others. When a person does not put the effort to provide clear answers, they are out of the race. I am looking for a person willing to do their homework.

Everyone knows someone who is associated with real estate. When you disclose to friends and family that you are house shopping, you might be bombarded with referrals. These should be avoided. When you contact a friend of a friend that is a real estate agent, you just lost all anonymity. Your real name will be entered into the provider databases and there is now a trail from you to the home you choose. I believe your chosen professional should never know your real name. That may sound harsh, but consider the following.

A client allowed a friend to be the buying agent on her behalf. The home was placed into a trust and her name was not present on the public county records. She placed the utilities in the name of the trust and did a great job of remaining private. Her friend entered my client's real name and details into the database owned by the large national chain realty association. After the purchase, my client began receiving junk mail at her home, addressed to her real name, asking her to refer others to the business that helped her during the purchase. A month later, she began receiving unsolicited mail offers for appliances and exterior cleaning services. The buying agent's company sold their customer list to third parties. My client is now exposed,

and can never fully repair the damage. If you want a truly private home, you must watch every step and never disclose your real name to anyone associated with the sale.

Let's assume that you have found a few homes you want to view and you have identified a real estate professional with whom you want to start working. Before you meet, you should have several things in order. I will list these individually including considerations for each.

Email: When you contact real estate professionals, assume that everything you provide to them will be shared publicly. They will register your email for unsolicited messages and share it within various marketing systems. I always create a ProtonMail email address for the sole purpose of the home purchase. It does not identify my name or the trust name. I keep it generic such as home.purchase@protonmail.com. The name associated with this account, which will be seen by recipients, is also generic such as "Homes". This is the only email I will use during the entire process, including closing paperwork. It will not be used anywhere else.

Phone: Your hired professional will want your phone number. This will also be entered into the databases owned by the company and shared with numerous third parties. I designate a VOIP number for this, and choose an area code associated with the general location. I will never use this number for any other personal purpose. I expect this number to become public.

Name: In my early attempts at purchasing an anonymous home, I was very restrictive over any information divulged to anyone. I found that telling someone, "I would rather not give you my name", was not well received. It also caused extra awkwardness during every encounter. I no longer do this. Instead, I am Michael Johnson. I keep it simple. No one has ever asked for identification during the house hunting process. This will happen closer to the closing, and we will deal with that later.

Current Location: Everyone wants to know where you currently live. Much of this is small talk in order to seem polite, but some is to identify the type of location you may desire. I always have a story ready for this. I usually go with, "I am renting in (nearby town) while I look for a new place". I avoid anything exotic such as Hawaii or anywhere else mildly interesting. If you get pushed for a specific address, have a nearby hotel address ready to go.

Current Employment: One of the first questions you will hear from your house hunter will be, "What do you do?" Again, this is small talk, but anything you say will be documented somehow. Most successful real estate professionals add this to your profile and use it when they need a reference from a specific industry. I recommend keeping it simple. I usually go with, "I work from home as an accountant. It's pretty boring, I add numbers all day". There is rarely a follow-up to this, and you just set the scene that someone will be home at all times when you move in. This can be a burglary deterrent when questionable subjects start asking about you.

Personal Interests: In general, I hate this type of small talk. Questions such as, "What do you do for fun?" are used to form a relationship. If I say that I play baseball, the other person believes he or she must mention baseball on occasion in order to build my trust and close the sale. This is typical in all areas of sales. I just say, "I'm doing it now!" and move on. I caution people to avoid saying too much. While it may seem acceptable to disclose your passions for classical piano and vegan food, you just made yourself quite a large needle in a small haystack. Keep it simple.

Faraday Bag: This one may be a bit on the paranoid side, but consider your cellular telephone usage while viewing homes of interest. If you subscribe to the 2-phone plan presented previously, you may want to prevent your device from connecting to cellular towers near your future home. This is especially true if your device is registered in your real name. When you enter a home address into your mapping application for directions, this is stored forever within some platforms. If you buy the home, in which you entered the address into your phone, you now have a small yet permanent connection from your device to your new home. I prefer to meet with my real estate people at their office, and then either ride with them or follow them in my own vehicle. My mobile device is in a Faraday bag during the entire hunt. If I want a photo of something, I ask my agent to photograph and email the images to me.

My last piece of advice is to rely on old-fashioned social engineering when necessary. If questions start to become invasive, turn them around and get the other person talking about themselves. When I am asked, "What is your rental address?", I reply with, "Hey, that reminds me, what do you think of the Tempe Heights neighborhood? Do you live near that area? Where would YOU move to?" That should get them on a different track. This can be applied to practically any topic. When asked, "What do you like to do on the weekends?", I return a question of "What is there to do around here? Where do you hang out?". This may take some practice, but will go a long way in your future of being private.

In regard to choosing a home, most of this decision will simply be personal choice. When I am assisting a client with a history of domestic abuse, I want him or her to feel safe and have some extra security protection. If my client is well-known, I may place more priority on privacy. Regardless of your situation, I ask you to consider the following privacy and safety issues.

Privacy from neighbors: Most people that reach out to me for help buying a home anonymously have a strong interest in privacy. I first look for privacy fences and windows which do not expose the inside to a direct view from the street. I don't want the interior to seem like the outside is watching in. Big windows and glass doorways are nice, until they are a security and privacy risk.

Garage to hide vehicle: Possessing a garage is vital for any home I will consider. This has nothing to do with the security of the vehicle(s). A properly garaged vehicle does not expose license plates to public view. Attached garages are best, as a vehicle can be loaded for a trip without the neighborhood knowing you are packing.

Interviews: This plays a large role in my selection of a home. The residents surrounding a home can give quite an indication of potential problems, or lack of. I usually conduct a search of the neighborhood on people search sites, identify the residents, and take a look at their social networks. This gives an overall vibe of the community and may identify any bad apples. Researching police reports online is also beneficial. If your area does not provide this, strike up a friendly conversation at the local police department and ask about that specific area. Finally, I place a lot of emphasis on my own "street walk" around the neighborhood.

When I was conducting my street walk for a client in northern Arizona, I encountered a neighbor mowing his grass. I asked if I could step on his property and we had a brief conversation. I asked about the neighborhood as a potential buyer, and he had nothing but great things to say. It turns out the vacant home for sale was the issue, and the entire neighborhood saturated local police with every witness of a drug sale or physical altercation at the residence. The problem-residents finally moved due to the pressure from a proud neighborhood. When searching for a home for a violence victim, I welcome concerned neighbors that are not afraid to get involved. My final question was, "What were their names?" The man responded, "I have no idea, we keep to ourselves for the most part out here, until you cause trouble". Perfect.

Assume now that you have found the ideal house. You have already established a trust as previously explained. You have a person you trust to serve as your trustee, preferably with a common last name different than yours. You have a notarized certification of trust at your disposal, which is signed by your trustee. You are ready to make an offer, and it is time to jump in.

During my initial explanation of my anonymous home strategy, I will assume you are paying cash. I know this just upset some readers. While most of my wealthy clients have spare cash to throw at a problem, the rest of us do not. I start with cash purchases because they are the easiest. I have never had any major obstacles in these scenarios. At the end of this section, I will discuss hurdles that enter into a home purchase when obtaining a mortgage. These will vary depending on your location and lender, but you have options in all situations.

The original offer and earnest money are fairly simple. The contract can be created using digital-only services such as DocuSign, and all of this will be performed by your real estate representative. You can state that you want the offer to be in the name of your trust, and that your trustee will digitally sign. You can use your previously given email address in order to

receive the links to the online documents. The earnest money can almost always be in the form of a cashier's check. This is usually a 1% deposit based on the offer price. If you back out without an acceptable reason, the seller can keep this money. The cashier's check does not identify you or your account and it is usually held by the chosen title company. The DocuSign electronic documents will arrive, and require the trustee to click "I accept" a few times. In optimal situations, the signature line only identifies the trust at this time, and not the trustee name. You can specify this to your representation.

Before I move on, I encourage you to research the title company before you commit to an offer. In many cases, the seller chooses the company to use, but you can request a different option if you are uncomfortable with the selection. I always call the chosen title company and ask the following questions.

- Can the deed be placed in the name of a trust?
- Does the trustee name need to appear on the deed?
- What documents will you need?
- I have a certification of trust, will that suffice?
- Is there any specific wording you need on the certification of trust?
- Can my trustee sign from a remote location?
- If you demand a "wet" signature, can this be notarized and sent via overnight mail?
- Will anyone need to be present at the closing?

I am looking for acceptable answers and an overall confidence in their ability to title a home in a trust. I have found a few title companies that were completely incompetent, which caused more problems for me. As the buyer, you have the power in this sale. Make sure you are comfortable with the title company selected for this transaction.

Some sellers will require a proof-of-funds letter. With a cash purchase, this is a document created by the bank holding the funds confirming that a specific amount of money (determined by you) is currently available in the account. I try to avoid these with the initial offer, but I am never surprised to see the request on the final acceptance. If this is required, I will explain bank accounts in trust names in a moment. If securing a loan, this is a document created by the lender acknowledging pre-approval for a specific amount.

After some negotiation, an offer is usually accepted by both the buyer and the seller. There will be several digital "signatures" during this process, all in the name of the trust, and preferably without the trustee name. Some title companies will insist that the trustee name is present, and the line will read similar to The Home Buying Trust, John Wilson, Trustee. This is acceptable, as this information will be needed at some point regardless. These documents should stay fairly private, but this data will be used for public documents eventually. Please

revisit "Choosing a Trustee" in the legal infrastructure chapter before you commit to someone.

Assume that you now have a contract for the house. The rush for inspections begins, and you need to schedule numerous people to visit your potential new home. This can feel quite invasive to a privacy-conscious person, and I see many people make numerous mistakes at this point. Any company that is hired will demand information from you. Furthermore, they will contact the title company and retrieve any details that it possesses. The service companies will abuse this data by sharing it with third parties, and you have almost no say in the matter. Anything you provide will eventually be public information. Approach with great caution, and consider the following incident which happened to a client in 2018.

My client hired a local home inspection service to inspect the entire house. She found a company with great reviews and felt confident in hiring the service, which she found online. The inspection company used a service called Porch for all reservations and billing. These online services make it easy for the contractor to focus on the job and not the logistics. While convenient for the workers, it is a privacy nightmare for you. The following five excerpts were taken directly from the porch.com privacy policy website.

"We may share your information when you consent or direct Porch to do so. Depending on the circumstances, consent may be expressed (i.e., you specifically agree either verbally, in writing or electronically) or implied."

"You consent to be contacted by these parties by telephone, email, mail, text (SMS) messaging, fax, or other reasonable means at any of the residential, cell or fax phone numbers or addresses you provide, even if they are listed on a national 'do not call' or 'do not contact' list. You agree that these communications may include prerecorded, artificially voiced or autodialed telemarketing messages, and that they may be monitored and recorded for quality assurance and other reasons."

"From time to time, we may partner with third parties to offer discounts, rewards or other programs or promotions. We may disclose the personal information of the participants in the programs to those business partners. …We will disclose your personal information to those business partners when you consent to that disclosure, including consent implied by your agreement to the applicable program rules."

"We may decide to sell, buy, merge or reorganize our own or other businesses, conduct a securities offering, or do a joint venture or other strategic transaction. We could also be involved in a bankruptcy, liquidation, dissolution or similar transaction. Any such transaction may involve disclosing personal and other information."

"We may share aggregated, non-personal data with service providers, advertisers or existing or potential business partners."

In summary, any information provided can (and likely will) be shared, sold, given, traded, or lost to any company that may have interest in you as a new homeowner. Deals like this are the reason that we all get bombarded with unsolicited mailings in relation to home ownership when we move into a new house. While some may enjoy the promotional material, we have a more important concern. The more your name and address are shared with marketing companies, the faster your information will appear publicly online. If you want to keep your name and address private, you have two obligations.

The first is to avoid companies like this. My client was able to track down a direct telephone number for this inspection service and politely requested to book an appointment directly. Instead of citing privacy concerns, she stated she was not tech savvy and couldn't figure out the website. The service obliged and conducted the work, submitting a paper invoice and happily accepting cash for the job. The second obligation is to expect every provided detail to be publicly released. Therefore, you will only provide the name of the trust as the customer. If you receive grief for this, tell the provider that the trust is paying for the work, and your name being present could delay payment.

Once the title company starts doing their work, they will probably request to see the entire trust document. This is an extreme violation of your privacy, and they may "record" it with the county. Remember, the entire trust outlines you as the grantor and beneficiary, and your desires for asset distribution when you die. No private or government organization should ever need that entire document. That is the purpose of the certification of trust as explained earlier. Provide a notarized copy of the certification of trust to your representation to give to the title company. The title company may also request a Statement of Authority signed by the trustee. This will be a form specific to each company, and allows them to continue their work in good faith that the trustee approves all of these actions. This may specify the address and timeline, and is acceptable. All of the future digital signature documents will likely display the trustee name after these documents are provided.

This brings up another important point. You should never need to deliver anything directly to the title company. In my purchases, I never step into a title company's office. They do not know what I look like. By not being present, you cannot be tricked into signing something or displaying identification. Allow your real estate broker to earn their commission and do all of the leg work.

Assume now that the inspections are acceptable and you are ready to proceed with the purchase. A closing date will have been set by the title company, and they will demand the remaining money to cover the purchase price of the home. When paying in cash, I always

recommend providing the funds a few days prior to the closing date. Some title companies want the check to "clear" before approving the transfer, especially when the situation is unique. This brings us to the next dilemma. How do you pay the title company anonymously?

This can get a bit tricky. The official answer is that you can never have 100% anonymity when buying a home with cash in America, even with the use of a trust. The exception might be homes under $25,000, but that is not very applicable to our situation. This is because there is always a paper trail of the financial exchange. You cannot show up with $300,000 in 100-dollar bills and walk away with the keys. Any check, even a cashier's check, can lead back to you. Therefore, our desire is to be PUBLICLY anonymous. If the IRS wants to prove you bought a specific home, they will succeed. They have the power of court orders to financial institutions. If a private investigator or journalist tries to determine your home address, we can make that extremely difficult, if not impossible.

When I began assisting with anonymous home purchases in 2015, I was able to present a cashier's check for practically any amount. This check was issued by the same bank that my clients used for personal accounts, but the check number was not directly associated with the client. The bank could disclose transaction data if provided a court order, which would identify the client, but the title company would have no details about the client's account. This worked for a couple of years until wire transfers became the mandatory procedure. Today, practically every title company will demand an electronic wire transfer for amounts over $25,000. Most companies claim this is due to fraud, but wire fraud is more abundant than check fraud. I believe that title companies demand wire transfers because it provides less liability than a check. It is easy to immediately confirm a transfer with the issuing bank.

I have given up my fight to provide a cashier's check for the home purchase. My last success was in 2017, and it was quite a struggle. Today, the only sales which accept cashier's checks are auctions of foreclosed properties. I see many bidders bring numerous checks in various amounts, such as $25,000, $50,000, and $100,000, in order to make immediate payment. There is less scrutiny on these lower purchase prices. When purchasing a home through a more traditional process, I provide the final purchase amount via wire transfer from a new account created in the name of the trust. This should be done with much thought, and please consider the privacy implications before submitting a wire.

A wire transfer is an electronic transfer of money. A traditional wire transfer goes from one bank or credit union to another using various computer networks. In order to send a wire transfer, you need specific instructions directly from the recipient (title company). These details are given to your bank, and the wire transfer request is prepared. You may be charged a small fee, and the transfer is almost immediate without a hold on the funds.

You must identify the account which will provide the funds. If you have the entire purchase price sitting in your personal checking account, a wire transfer can send the money straight to the title company. However, this process will also send your name and account details. Any information provided to the title company is likely to be filed with the county, and can become public record. Therefore, this is a bad idea. My preference is to create a new account within the name of the trust.

It can be convenient to ask your current personal bank to create a secondary account for your trust in order to send a wire transfer from it instead of your personal checking. This can be a mistake. Consider the financial risk company Early Warning. Early Warning delivers payment and risk solutions to financial institutions nationwide. In 2017, I requested my own consumer report from them. It clearly identified all of my checking, savings, and investment accounts. It easily connected all of the accounts to me, and provided details for every deposit, withdrawal, and payment associated with each account. Early Warning shares this data with over 2,500 financial institutions and unknown third parties. In other words, this company knows when you add an account, all payment details including wire transfers, and historic balances since the account was opened.

My preference is to open a new account at a local credit union in the name of the trust. This should be done in advance of placing an offer on a home. While this institution may participate in systems that share account details, there will be a degree of separation from your personal accounts. Your procedure for this will vary based on the trustee of your trust. There are two routes I recommend.

- If YOU are the trustee of your trust, you can create this account yourself. You will need to provide your DOB, SSN, and identification. Make sure the account is only in the name of the trust, and that your name does not appear in the title. This account is obviously associated with you, but could be used as a layer of privacy protection when only disclosing the name of the trust.
- If SOMEONE ELSE is the trustee of your trust, you cannot open the account yourself. Banks and credit unions will want to see the trust documents and will only allow the trustee to create the account. Obviously, they will want the DOB, SSN, and government identification from the trustee. This can be very uncomfortable for a trustee, unless it is a close family member or spouse. Consider making yourself the trustee before opening the account, and then amending the trust to assign someone else as trustee during the closing process. This will be explained in a moment.

Both of these options may seem sloppy and they both possess privacy exposure. Neither are perfect, but they may be your only options. I cannot guide you toward your best choice, but I can offer a detailed example of the actions taken by a recent client. I have included a modified timeline to show the approximate dates when each step was taken on the following page.

January 1, 2018: My client created her trust, assigning herself as the trustee and beneficiary.

January 2, 2018: My client opened a checking account, in the name of the trust, with a local credit union. The account is associated with her SSN. She complied with all Know Your Customer (KYC) laws. Instead of the entire trust document, she only provided the certification of trust. She deposited enough funds to pay any potential earnest money requirements via a cashier's check from another bank.

January 10, 2018: My client identifies the home she desires, places an offer from the trust name only, obtains a cashier's check in the name of the trust from the trust checking account as earnest money, and digitally signs the offer in the name of the trust without a specified trustee. The offer is accepted.

January 11, 2018: My client transfers the approximate funds required for the complete purchase from the bank associated with her personal checking account to the new trust account, via cashier's check, from the original bank. This will require 2-3 days to clear.

January 15, 2018: My client is informed of the final amount due to the title company to purchase the home and is given wire transfer instructions. She verifies the deposit into the trust account. The payment is due before the closing date on January 30, 2018.

January 16, 2018: My client provides the wire transfer instructions to her credit union. A transfer for the final purchase price is issued and received at the title company. She made sure that only the name of the trust appeared on the wire, and that her name was not present within the digital transaction.

January 17, 2018: My client amends her trust and assigns the role of trustee to her niece, who is a trusted family member with a different last name.

January 20, 2018: My client's niece provides a real "wet" signature on the title company's statement of authority document and my client provides a notarized copy of the certification of trust document declaring her niece as the trustee, and signed by her niece. These two documents allow the niece to digitally sign at closing.

January 30, 2018: My client's niece remotely executes the digital signature for the closing and my client now owns the home.

January 31, 2018: My client amends the trust, re-assigning herself as the trustee. Some may choose to postpone this until utilities are activated.

As another reminder, I am not an attorney. In this situation, my client created and controls her trust. She made herself the trustee in order to open a checking account in the trust's name. This will be beneficial during utility activation. Before signing any paperwork with the title company or providing trust documents, she assigned her niece as the trustee. This gives the niece the full power to sign on behalf of the trust. The only name the title company knows is that of the niece. The client is still invisible to the title company.

This section has been simplified, demonstrating a successful execution with a cash purchase. There are always hurdles faced throughout an anonymous home purchase. The biggest roadblock you will face is when obtaining a loan for a home. You are now at the mercy of the lender in regard to titling the home in the name of a trust. Be selective about your choice of lender. During the initial conversation, advise that you wish to place the home in the name of your trust for estate planning purposes. The first response will likely be positive, but you should push the issue more. I recommend the following series of questions to a potential lender.

Can I place the home in the name of my trust at the time of purchase? This wording is important. Some lenders will insist you place the home in your name at the time of purchase with the option to change the deed to the trust after purchase or after the loan is repaid. Titling your home in your name for a single day is enough to expose your address to the internet forever. Most lenders agree to this without verifying with the companies to which they will resell the mortgage.

Can the trustee be someone other than myself? This will be met with resistance. I have witnessed larger lenders, such as Fannie Mae, reject this while local banks allowed it. If you want to keep your name off the county record, it will be important to have a trustee other than yourself. Make this requirement clear from the start.

Does the trustee need to be a co-signer of the loan? Lenders which have allowed a third-party trustee later demanded that the person be listed within the loan. This is unfair to the trustee and is inappropriate. Obtain a clear answer on this ahead of time.

Overall, a lender will know everything about you, including your SSN and DOB. In order to give you a line of credit, a hard pull will be conducted on your credit history. They will know the address of your home and the name of your trust. There is no way around this when obtaining a loan. However, they will probably not share these details publicly. The concern is a data breach or third party which has access to this data. This is why I focus on smaller credit unions and banks. Ask whether the institution resells their loans or keeps them in-house. While local banks which provide their own loans are diminishing, they still exist. These will place much less scrutiny on the use of a trust.

Paying with cash will always be easiest and most private, but possessing a layer of privacy by using a trust during the loan process is also helpful. For most clients, the goal is to stop home addresses from being published on the internet. This can be achieved whether obtaining a loan or paying cash. Only you can decide the approach which is most realistic for you.

Tax Record Exclusion

I have had a handful of clients which possess an affiliation with law enforcement who desire privacy in regard to public property tax records. If your home is titled in your real name, many counties offer an option to request these details be hidden from public view. This requires completion of a specific form and a letter from your employer stating that you work in law enforcement. The only time I recommend this is when you will not be placing the home into the name of a trust. If you are purchasing an anonymous home, I believe this option is an awful idea. In a way, you are making yourself a larger target. A rogue employee, or poor security protocols at the county offices, could expose you and your address. Furthermore, if you are the only home in your neighborhood with missing tax records, you must be someone special. I much prefer proper titling into a trust. You then need no additional "protection", which may actually backfire on you.

USPS Issues

In 2018, I helped a client purchase an anonymous home in a rural area of Missouri. After he moved into the home, he realized there was no mailbox on the property. He soon discovered that the entire neighborhood collected mail at one central group of mailboxes further down the road. These boxes required a key, which my client did not possess. A call to the post office resulted in a demand for a list of occupants. This was met with immediate concern from the client. I have seen this many times, and the solution has been surprisingly easy. I recommend having your trustee contact the local post office. The trustee should state that he or she is not currently residing at the property, but that someone can be sent to the local office with the closing paperwork from the title company clearly identifying the trust and trustee name. The owner can then take in these details without the need to provide any type of identification.

Since the USPS is a government agency, we want to be cautious to never lie or give inaccurate details. Showing them the closing paperwork, identifying the full name of the trust and trustee, should be sufficient to add these details to the local carrier's roster. In my experience, possessing the original closing paperwork is enough to be given a key to the mailbox. I encourage the trustee to be listed on the USPS roster in order to accept any mail in that name. Often, property tax bills and utilities will be mailed to the trustee's name instead of the actual trust. The next hurdles include utilities and various home services. The next chapter will present numerous solutions to keep your name out of marketing systems which sell your data.

Children

Children present a new hurdle in the desire for an anonymous home. If your children are home schooled, you likely have no issues. If you reside in an urban area with competitive schools, this could present concern. Many schools demand proof of residency in order to eliminate children from other areas who are trying to avoid their own troubled schools. Overall, I recommend registering your children within the appropriate schools local to your home. However, do not provide your actual home address. This will be placed into many records, including some that will likely become publicly available online. I have found county schools to be much less restrictive about residency requirements than city schools. You will be constantly pressured to provide your home address, and the following ideas may buy you enough time until they stop requesting your personal details.

Obtain a local UPS box and provide that address as a street address. If questioned, state that you are in the process of building a home in a nearby neighborhood. Make sure your actual home address and the UPS store address are both within the boundaries for the chosen school. This keeps your actions legal. If asked where you are staying, provide a hotel address within this same area, and clarify that you want the UPS address used for all mailings. In my experience, you will only receive resistance if that school is strict about blocking non-local students from attending. Make sure that the school you choose is also funded with your property tax payment. This provides additional legal compliance if you should ever be accused of fraudulently enrolling your child into a specific school.

The use of a legal guardian, such as a grandmother, may be appropriate for you. A child can be associated with a legal guardian within school records and that person can sign documents when required. This may not offer a strong layer of protection, but could keep you off school records which will likely become publicly available. In my experience, private schools are much less demanding about home address verification, as they are directly funded by you. Most private schools do not have a specific residency requirement, and will accept a UPS address as the primary residence.

Bringing children into an invisible home can carry many more issues into your life. This will likely generate several long discussions about cellular telephone usage, internet habits, friends in the home, alias names, employment, and the protection of the details you have hidden. I hope that the overall lessons within this book assist with these discussions and decisions. I can assure you that many of my clients lead invisible lives, even with children in the home. This will require more effort on your behalf, but the work is worth the reward. As an added bonus, creating privacy awareness with your children at a young age may provide many future benefits once they obtain their own independence and enter the world of data mining, credit abuse, and numerous other privacy violations.

Neighbors

The final concern within this chapter is your neighbors. Most residents in your new neighborhood will want to get to know you. They likely have great intentions and simply want to be good neighbors. While some may be nosier than others, everyone in your neighborhood is a potential threat toward your privacy. I may not take this harsh of a stance if it were a pre-internet era. Today, we are at risk of online exposure everywhere we turn.

During the home selection process, I mentioned how I monitor Facebook groups in order to identify potential problems before moving into a neighborhood. These same groups are now a threat toward your anonymity. Your neighbors will post any gossip they hear within these groups and use them as an outlet to vent frustrations with other neighbors. My best advice is to stay off the minds of these people. Don't speed through the neighborhood, keep your property maintained, and keep to yourself. These three suggestions will keep you out of the majority of the drama within online groups.

The next concern is new privacy invasion companies such as Nextdoor.com. Nextdoor is a social networking service for neighborhoods. Users of Nextdoor submit their real names and addresses to the website and posts made are available only to other Nextdoor members living in the same neighborhood. The premise seems like it offers a small layer of privacy by allowing people to communicate with neighbors without the content being publicly visible to the rest of the internet. However, I am very concerned with the amount of detail being collected by Nextdoor. First, let's look at three excerpts of the privacy policy.

- "We share information with service providers, affiliates, partners, and other third parties where it is necessary to perform the Member Agreement, to provide the Services, or for any other purposes described in the Policy."
- "We may share your personal information with certain third-party service providers to help us operate, provide, improve, understand, customize, support, and market our Services."
- "We share some aggregated information about our neighborhoods with government agency members and other organizational members."

In other words, much like every data mining company in America, they have the right to do practically anything they want with your information. After moving into my anonymous home, I received a letter in the mail from Nextdoor. It was an invite to join the group assigned to my neighborhood, and it specified the neighbor (full name and address) who requested Nextdoor to contact me. This already felt invasive, but I played along.

The invite included a specific code which allowed me to join Nextdoor without providing address verification. I entered the code on the Nextdoor website, and it immediately populated

my entire home address (but no name). The code was unique to my house. Nextdoor then demanded to know the name of the primary occupant of the home. I entered J Doe, and I was declined. An error message notified me that the system required a full name in order to complete the registration. I entered John Doe and was declined again. I was informed that real names must be entered, and I began to wonder how people would join if their name was really John Doe. I settled on John Williams and I was allowed to proceed.

Nextdoor asked me to complete a profile about myself which included interests, hobbies, and my overall reason for joining Nextdoor. Fortunately, there was an option to skip all of these. They then requested the full names and email addresses of all occupants, which I skipped. I was then prompted with a screen telling me I needed to invite one friend to Nextdoor, and I was offered the option for Nextdoor to connect to my contacts in order to easily select someone. Skip. Nextdoor then displayed all of the local addresses in my neighborhood which had not enrolled in the service, and asked if they could send invite letters to each of them on my behalf (disclosing my full name and address). Skip. Finally, they pushed me to install the Nextdoor mobile app (in order to collect more details from my device), which I declined. By default, all local users now see the email and full address in my profile.

I realize I am a bit paranoid, but this smells like a data mining company to me. Imagine all of the extremely accurate information they receive from the occupants of a household which is not available anywhere else. I suspect that we will see this data emerge into other people search companies. The email address I provided for my profile was unique to this service. I eagerly watch for it to appear within other online repositories. I will update this on my podcast if anything should surface.

I never posted to the neighborhood group on Nextdoor, but an announcement was made that I had joined. The entire group received a public message on the community wall stating my full (alias) name and street of residence. I then began receiving unsolicited messages ranging from "Welcome to the neighborhood" to offers for home improvement. Reading through the comments, I observed the usual offenders. Most were people complaining about speeders and ugly properties. On one post, the commenter identified the license plate of a vehicle which upset her, and a response identified the name and address of the owner. These groups are your next threat, and can quickly unravel all of your privacy strategies protecting you.

While updating this chapter in April of 2020, I logged in to my Nextdoor accounts in order to identify the ways in which communities were embracing this technology during the COVID-19 pandemic. I was not surprised to see posts shaming neighbors, including full names and addresses, who were not "social-distancing" correctly. However, most of the content was for the purpose of spreading unverified information and conspiracies associated with the area surrounding my neighborhood. It was a mess.

Private License Plate Readers

There are additional emerging threats to your privacy associated with your neighborhood. In early 2019, a client reached out with a new concern. She was advised by her neighborhood watch president that he had installed license plate readers at all entrances to the neighborhood, and that he was logging all vehicles, along with dates and times, coming and going. She asked me if this was legal, and if I had never heard of such a scenario. I identified a company that was marketing license plate readers to neighborhoods, and called them to get more details. This call was included in my podcast about the issue (Episode 118: How Neighborhood Watch Watches You).

I learned that many neighborhoods were installing license plate readers in response to property crimes occurring within the area. The cameras collected video footage of each vehicle entering and leaving the neighborhood, along with a text translation of each license plate. The administrator of the system, which is usually the neighbor who purchases the cameras, receives a daily log of all vehicle activity. He or she can pass along any desired details to the police if a crime occurred. Furthermore, this person can log in to a website and search a specific license plate in order to see a pattern of activity. I immediately began researching the legal implications of destroying such cameras. Hint … it is illegal to damage private property.

I am sure most of the neighborhood watch participants who install these systems have good intent. They want to catch bad guys stealing things. However, this power can be quickly abused. When a neighbor wants to know when you came home last night, he or she has the ability. Do the logs show the average time you leave every weekday morning and return in the afternoon? This tells me the best time to snoop around your property. Did you have a friend follow you home late on a Saturday night? I now have a permanent record of this visit. Did the vehicle leave early on Sunday? I now have some new gossip for the neighborhood.

It should be noted that these systems do not verify collected data with registration information. The system does not know your name or address. It can only document the letters and numbers on the registration plate. However, your neighborhood watch administrator could easily associate each plate with a specific neighbor's address with a simple drive through the streets. Anyone who desires this type of system to monitor the neighborhood is the type of person who keeps a record of residents' vehicles.

I would never consider living in a neighborhood which possessed this type of monitoring. If a system were proposed, I would fight it and encourage other neighbors to join the resistance. If a system is legally installed regardless of your desires, you will find yourself in the same scenario as my client. My advice to her was simple, yet annoying. I told her she should consider removing her license plates before entering her own neighborhood. This is likely illegal, but with minimal chance of being detected. Please let me explain.

You must legally display valid vehicle registration plates while on any public road. This usually includes the roads within your neighborhood. If my neighborhood entrance possessed license plate readers, I would identify a safe place to pull over before reaching the entrance. I would then remove the plates and proceed directly to my home. After leaving the neighborhood, I would use the same location to re-attach my plates to the vehicle. Technically, I would be illegally driving the vehicle for a few minutes within my own neighborhood. If I were stopped by the police, which would be extremely rare, I would politely explain my reasons, display my plates to the officer, and accept any citation issued to me.

You may be thinking that carrying a screwdriver and removing both registrations plates every day would become quite a chore. You are correct, but the action of removing the plates can be made much easier. My vehicle plates do not attach via screws. I use a magnetic plate holder which requires over 25 pounds of pull in order to remove it. These can be found on Amazon (https://amzn.to/3bWXyDF). I can easily remove my plates by simply giving them a brisk tug and replace them by pressing them against the vehicle.

Please note that these will only work if your plate attaches to an area with a metal backing. I have a vehicle which possesses a plastic well for both the front and rear plates. Therefore, I place the magnetic holders (with plates) above the license plate well where I have access to a metal surface. Your plates must simply be visible, and there is no law requiring you to use the designated attachment areas. Why would I do all of this? There are several reasons.

My newest excuse for these removable plates is the growing presence of neighborhood watch vehicle trackers as previously discussed. I also prefer to remove my plates if my vehicle will be on my property but not in my garage. This prevents Automated License Plate Readers (ALPRs) installed on many police cars, tow trucks, taxis, and other service vehicles from associating my vehicle registration with my home address. These magnetic holders are also convenient when parking in private garages, airport lots, and large shopping centers.

One concern for a magnetic license plate holder is the increased possibility of theft. This is not a concern to me. If a criminal really wants my license plate, he or she likely has immediate access to a flathead screwdriver. A traditional plate with screws will not deter a thief. Most thieves will not notice my magnetic holder from a distance. When my vehicle is on private property and out of my site for a long period of time, I remove my plates anyway.

Many readers might consider displaying their license plates from inside the vehicle. A front plate resting in the dash of the vehicle and the rear plate attached to the interior of a rear window may seem like a good idea. It is not. Almost every state specifically requires registration plates to be attached to the exterior of the vehicle. I never encourage people to execute illegal methods which may bring more attention from law enforcement. This can ruin privacy strategies quicker than anything else.

I hesitantly present one additional option which may keep your license plates private. There are numerous "plate flippers" and "plate covers" online which allow you to hide your plate remotely from within the vehicle. An internal button instructs the frames holding your plates to flip the plate over and display only the black back-side of the holder or lower a cover. Executing this while traveling on any public road would be considered illegal. I believe flipping your plates while on private property could be allowed. This decreases the chances of plate theft and hides your vehicle registration while parked. This may be illegal in your state, depending on your usage, but I could not locate any laws specifically preventing such a device.

The next concern is new optical character recognition (OCR) software being embedded into existing home surveillance systems. One such offering, titled Rekor Systems, launched a service called "Watchman Home". This software can turn nearly any existing home security camera into a license plate recognition device without the loss of the original security camera functionality. It can be integrated into smart home systems to automatically recognize specific vehicles, and attaches to internet-connected devices for remote monitoring. Any of your neighbors can log in to their own portal to see the entire history of all vehicles traveling near their home. The cost is $5 per month, and there are no physical indications of it being used.

I believe we will see neighborhood vehicle tracking cameras become the standard within the next ten years. The hardware is very affordable and the software costs will decrease with heavier use. Many of your neighbors already possess security cameras facing the street, and possibly your home. Because of this, and the popularity of online groups such as Nextdoor which allow abuse of collected data, I ask you to consider what information you will provide to your new neighbors. Expect that any details could become public within an internet group. If you upset someone, do you want your full details shared, including your travel history?

I insist on always providing an alias name and backstory to my neighbors. They all call me John. They believe I travel the country applying software patches to large commercial heating systems. I am boring to them and they do not think of me often. It does not change my relationship with them, but it makes me worry less when someone decides to mention me on the internet. No one knows my true name, license plate, or background. I stay away from any neighbors fueled by drama. If I am mentioned or documented within their social networks, the data will not compromise my privacy as it will not be accurate. This may seem extreme to most. However, there are no "re-dos" when sharing personal details with a neighbor. Anything provided will be repeated, embellished, and exposed. Choose wisely.

Finally, always remember the amount of effort which was required to obtain your private home. I doubt you want to unnecessarily repeat that process with a new property because of a small mistake which disclosed your true identity. Spend considerable time creating your new alias which will be presented to neighbors. Rehearse and repeat before "going live".

Nomad Home Ownership

You may have some confusion about how the privacy benefits of nomad residency, as explained previously, can be combined with home ownership. There are countless scenarios which legally allow nomad residency while owning a home, and likely as many which do not. I am not an attorney, and I could never acknowledge every unique situation, but I have opinions on many common scenarios which I encounter often. I ask you to consider the following situations which I have witnessed during consultations with clients.

A client became a nomad through Texas while leaving an abusive relationship. She eventually decided to purchase a primary home in Texas. The home was titled to a trust and her name was never associated with the purchase. She is employed in Texas, and her employer only knows her PMB address. She is legally a Texas resident and has no issues with the government by only using the PMB address. This could be replicated with South Dakota or Florida.

A client became a nomad through South Dakota. She later purchased a home in California, titled to a trust. She lives in this home full-time and owns no other properties. She never rents another home or lodging. Eventually, California will demand that she become an official resident or face steep fines. Legally, she should become a California resident and surrender her South Dakota license.

A client became a nomad through Texas and traveled the world in an RV for two years. He later purchased a home anonymously in Washington, but kept the RV. He continues to spend winters traveling through southern states and a few months in summer at his home in Washington. As a full-time traveler, he meets the requirements of nomad residency from Texas and calls his RV his "home". Washington does not have a state income tax, so he would not need to file a tax return to that state for any income earned while inside the state.

A retired client became a nomad through Texas and later purchased two homes in the name of his trust in other states. He does not spend more than a few months per year (total) in either home. He travels most of the year. He chose to keep his Texas nomad residency and calls his PMB "home". If pushed by either state of his homes, he could prove he spends minimal time in that state.

A client became a nomad through South Dakota. She later purchased a home in New York, titled to a trust. This is not her "primary" home as she travels often as part of her employment. She spends more nights away from her home than inside it. She calls South Dakota her domicile state. She spends much of her time in California as an actress, but owns no property there. Both California and New York could argue that she should be a resident of their state. She files a California tax return to claim her California income. She never works in New York and files no return there. This is a bit of a grey area, and should be discussed with an attorney.

Remember that you technically do not "own" your home. Your trust or LLC owns it, and you are the beneficiary. However, you should be cautious of state income taxes. If you earn money while physically inside a state with income tax, you owe your share. I have many clients who are legal nomads but spend much of their time in tax-aggressive states such as California. They make sure to possess a CMRA mailing address in California, and use it on their state tax returns, which claim all income earned while in the state.

Personally, I never recommend home ownership, even titled to a trust, in states such as California and New York, while trying to maintain nomad residency in Texas or South Dakota. It will catch up to you and you will face legal scrutiny from state government. It is simply not worth the risk or hassle. If you plan to live full-time within any state, you should be a resident of that state. If you can justify nomad residency due to extensive travel or multiple homes and an RV, then you may qualify. Don't make this decision lightly.

In my experience, states without income tax on wages such as Alaska, Florida, New Hampshire, Nevada, South Dakota, Tennessee, Texas, Washington, and Wyoming are less concerned with nomads being in their states. High-income states such as California, Hawaii, Illinois, New Jersey, New York, and Washington D.C. are always looking for residents who are not paying their share of state taxes. If you purchase a home in a non-nomad state, research the driver's license address requirements and apply the lessons throughout this book toward that situation. Most states simply want their tax, transportation, and other revenue from their residents. Keep them happy and live your anonymous life without scrutiny.

Selling Your Home

While you can get away without an SSN during the purchase of your home, it will likely be required when you sell it. This is because the title companies are required to report income from a home sale and must associate it with a specific SSN or EIN. The IRS requires you to pay taxes on income from a home sale if it exceeds a specific threshold. Most people are exempt from this taxation if the home was their primary residence, but title companies will insist on an SSN or EIN for the submission. I don't worry much about this, but I have a few rules for myself and my clients.

First, I only place a home for sale once I am completely out of it. I do not want strangers inside my home without me being present. I do not want any real estate professional to have access to my home at any time thanks to digital locks which can be opened with a smartphone. Once I am gone with no plans on living in the home again, I no longer care about the number of people entering and viewing the house.

Once I have moved to another anonymous location, I have no objection associating my name and SSN with the purchase of the previous home. I sold my house in 2015 which had no

connection to me. It was in the name of a trust. During the closing process, I provided the trust documentation disclosing me as the beneficiary. My Trustee provided a fresh signature. I provided my SSN to the title company for the check to be issued and confirmed a trust checking account associated with my true identity. There is now a trail from me to the residence, but I no longer live there.

International Considerations: Purchasing an anonymous home in America can present many complications, but is almost always possible. Some countries possess stronger privacy laws which do not make owner information public, and decrease much risk of associating your home to your true name. Some countries insist on documentation of the owners and occupants of every home, which can present more concerning problems. Please use the methods presented here in order to identify equivalent privacy strategies within your own country. I have never encountered a country which forbid home ownership by an entity such as a business or trust. If you do, consider the use of a trusted nominee for the documentation, but pay close attention to all fine print. Stay legal, but stay private.

Final Considerations

I have witnessed rare situations where a state demands to know a trust's beneficiary or director during the home purchase process. These demands are typically enforced by the title company. While an estate attorney can help you navigate this intrusion, consider the following. An LLC can be the beneficiary of a trust. As the grantor of a trust, you can temporarily assign another person as the director before closing, and reassign yourself as director after. We can usually find privacy strategy loopholes any time a state begins to tighten their controls.

Finally, any future homes should not use the same trust as any previous houses. A new home is a perfect opportunity for a fresh start, and allows you the freedom to disclose your true identity with any previous purchases. Since the names of each trust, along with previous and current addresses, will be publicly available, someone could match your old home with the new house if the same trust is used. While this is unlikely to happen, do not take any shortcuts. The extra effort of establishing a new trust is justified.

Chapter Nine

Anonymous Utilities, Services, & Payments

Assume that you have purchased your home privately. You have a "safe house" in which you can sleep well at night, without worry of any current or future adversaries showing up unannounced. You have completed a vital step, but now you have many smaller hurdles to conquer. Eliminating your name from the county records and public deed prevent much of the online scraping of public information. However, utilities and services are your next enemy. The moment you provide your name and SSN to a utility company for a "soft pull" of your credit, these details, including your new address, are shared with numerous data mining companies. I tested this in 2015.

I had just moved into a short-term rental which had no association to my real name. A former colleague owned the home, which had been vacant. I paid cash in advance and he handed me the keys. I only planned on staying a few months, so I was not extremely concerned with long-term privacy. I set up anonymous utilities, as explained here, with the exception of the power company. This was in California, and the power company was a government entity. This city provided its own power services. I was a bit new to the extreme privacy game and I was cautious not to provide any inaccurate information. I activated service with my true name and DOB. Within 60 days, my home address appeared associated with my name on a consumer information report available to third-party credit companies. I was burned. I expected this, and didn't think much of it, as I was moving soon. Today, I would never repeat that mistake.

If you are not diligent about possessing anonymous utilities, your hard work purchasing a private home will have been wasted effort. Many power companies, insurance providers, and household services supplement their profits by sharing customer data with third parties. My rule is to never associate my true name with my home address in any way. This includes any service that has a connection to my home. This chapter will explain several options to help you create your own anonymous payments strategy.

First, we need a way to make anonymous payments. I recommend a multiple-tiered approach. You should always have numerous options for payments available at any time. I have placed them in order of most desirable to least.

- **Cash**: This may seem obvious, but cash is your most anonymous payment source. I recommend that all clients maintain a steady supply of cash in the house in a secure location. Any service that accepts cash should receive it as a priority. Most clients make monthly trips to a bank branch a few cities away and make a withdrawal large enough to meet the demands for the month. I never suggest visiting a bank branch within or near your city of residence. This creates a pattern that can identify a great starting point to find you. Personally, I only withdraw money while traveling, and almost always outside of my home state. Cash leaves no digital trail, aside from video surveillance and fingerprints.

- **Prepaid Cards**: In previous books, I spoke highly of a specific line of prepaid cards. Today, I do not have much preference. These will only be used for in-store purchases, and never online. In order to use any prepaid card on the internet, you must first register the card to your SSN. If you only use them in stores, no registration is required. I look for cards that are NOT reloadable, and display wording similar to "gift card". I prefer options which can store at least $500 to minimize the purchase fees for each card. Prepaid cards leave no absolute digital trail to you if purchased with cash, aside from video surveillance, fingerprints, and transaction histories. Transaction history is stored forever, and purchases with the same card can be identified and analyzed. In a moment I will explain how this compromised a client.

- **Privacy.com**: This is a requirement for me and almost every client. This free service allows you to possess unlimited unique debit card numbers which can be attached to a specific vendor. Payments can include any name and billing address desired. Full details will be explained in a moment. There is obviously a connection to you, but it is not visible to the merchant.

- **Trust/LLC Checks**: Limited use of checks can be beneficial. Your bank can issue checks with the LLC or trust name without your name appearing anywhere. This creates a strong trail to you, but may be required on occasion, as detailed later. These are directly connected to your SSN, but the merchant does not see this association.

- **Alias Credit Card**: This may exceed the comfort zone of some readers, but it can be helpful when a true credit card is required. This was previously mentioned in the temporary housing chapter, and will apply to a few payment strategies. I will discuss additional related options in this chapter. This is the least private of all options, as the number is identical to your personal credit card number. Credit agencies will have immediate access to this connection, as will merchants if you use both personal and alias cards.

Prepaid Cards

There is a common misconception about prepaid credit cards being anonymous. While they can offer a great layer of privacy, any digital card payment is going to leave some trail. I am very cautious about the original purchase location and any use near my home. It is also vital to keep possession of all cards, even after the balance has been spent. Leakage of the card or account details can immediately expose your purchase history and could jeopardize the privacy of your home address. I will explain with the following details from an experience with a client in 2018.

An important part of any complete privacy reboot includes continuous testing. You might purchase an anonymous home with 100% success. However, what happens after a year or two? Are you still private? Did your name and address leak onto the internet? By constantly testing our strategies, we can have more confidence that we have succeeded. In this case, my client reached out to me, through her attorney, in order to conduct an assessment of her overall privacy. She lived in a home titled to a trust, and never associated her true name to her address. She followed all of the rules set forth in this book, and was doing everything correctly. Her threat model was high. She had a stalker who went to great lengths to track her. When he found her in the past, he violently assaulted her and destroyed her home. I was happy to see her testing her privacy strategy.

I confirmed with the attorney that I had full consent to attack her privacy strategy in any way I desired. I then contacted her directly and made sure she had truly invited this activity. Once everything was in writing, I began my attempts. I started with the easy stuff, such as people search sites, data mining services, and public records. Even with my inside knowledge of her home address, I was unable to find anything concerning. I then tried to connect a cellular account to her, but was unsuccessful. My attempts to gain access to any digital accounts using recycled credentials failed. It was obvious she had done a great job maintaining her new lifestyle. It was time to step things up a bit, using a recycled tactic that helped in a previous situation.

In 2017, I was tasked with a cheating spouse investigation. I knew the name and address of the target, and my job was to determine if he was having an affair. I purchased a prepaid credit card from a grocery store and shipped it to the target. I claimed that he had won the $250 gift card when he completed an online survey several months prior. Even if he was suspicious of the story, very few people will turn down free money. This is especially true for people hiding another life from their family. Before shipping the card, I documented the details including card number, expiration, security code, and website to check the balance. I checked the card transactions every day on the card's website. I only needed to provide the card number, expiration, and security code in order to have full access to the history. After a few days, it was used at a Chili's restaurant a few towns away from his home. A few nights later, it was

used at the same place. While monitoring the activity, I saw a pattern of use at the same Chili's every Tuesday and Thursday evening. This was where he was meeting his mistress. I provided this information to a local private investigator who captured photos of the two people eating, and later doing other things in the suspect's vehicle in the parking lot.

I borrowed heavily from this playbook for my new client. A condition of her job was that she must possess a LinkedIn profile, claiming employment from the company which hired her. It is a global company, so she did not need to provide any city or state of residence and employment. However, it was my start. I purchased a $100 gift credit card and placed it into a "Thank you" card. Inside the card, I wrote a small note thanking her for attending a conference at which she recently made an appearance on behalf of her company. I found evidence of this within an online roster of participants for the conference. I mailed this card to her name addressed to the headquarters of her company. I knew this would cause a delay, but that she would likely receive the card within an internal mail system. Nine days later, I saw activity on the card.

She used the card as payment at a gas station and later a Starbucks. This provided me a general area of her residence. Since I already knew her address, I knew I was on the right track. However, this would not necessarily expose her home if these actions had been conducted by her adversary. I patiently waited until she gave me the single purchase that I needed in order to connect her to her home. After logging in to the card's website with the card details, I saw a new purchase to a pest control vendor. A quick search of this business revealed that they offer in-home pest services such as spraying poisons to kill various critters. A documentation on the purchase made me believe that the card was swiped through a Square branded card reader, which allows people to accept credit card payment with their mobile device while on-site at an inspection. The purchase also displayed the transaction number, which could be used to track the purchase to an account.

I contacted the pest service and stated that I was in charge of purchasing for a small company and was attempting to identify a payment made for pest services. I provided the transaction number visible on the card's history to the employee and asked if she could tell me which property made the purchase in order to update my records. She immediately provided my client's alias name and home address. I thanked her for the time and ended the call. I had made the connection. I had exposed her home address.

You may think this tactic unfair, but her stalker is savvy and would never hesitate doing something like this or even worse. I don't place any fault on her for using the card. I had previously taught her to never use her real credit card for any home purchases and to only use a prepaid gift card or Privacy.com when absolutely necessary. What I failed to stress was the importance of avoiding the use of any gift cards associated with her name in connection to the home. I take full responsibility. She now knows to watch out for this type of attack.

The lesson here is that prepaid credit cards are great when needed, but still carry risk. In most situations, cash could have been used instead. Every credit or debit card maintains a permanent history of all transactions. Even though my client never associated her name with the purchases, I could still see a pattern of behavior. When it was used at the same Starbucks every day for a week, that makes me assume she lives in a specific neighborhood. This could lead me to more intrusive behaviors in order to identify her home. This may all seem far-fetched for some, but these attempts are the every-day reality for my clients.

My client was not upset at the trickery and seemed grateful to know about the potential exposure. On a more interesting note, she now uses this tactic to monitor her young son. She gives him prepaid cards as holiday gifts and monitors the locations where he spends the money. She assures me it is only to make sure he is not visiting shady places or potentially exposing the family any further. You may disagree with this type of behavior, but I respect her freedom to exercise her powers as a parent of a young teenager as she wishes.

My last guidance on prepaid cards is to use them sparingly and erratically. I only use one when I have no cash or cannot pay in cash. I purchase the cards while I am traveling in order to prevent the exposure of my local grocery store. I keep several cards in my possession at all times and label them with my own identification system. The following are examples.

01: This is a "Travel" card which is only used while I am away from home. The purchase history contains transactions from several states and has very little identifiable pattern. It is never used near my home.

02: This is my "Home" card which is only used when absolutely necessary in my home state. I never use it within the city where I live, but I have used it during local outings and errands. It has very minimal use, as I rely on cash when near my home. An example of usage would be a merchant which will not accept cash, such as a local utility. This card is purchased with cash from a local convenience store with an outdated video surveillance system which only stores ten days' worth of video.

03: This is a reserve card with no usage. It is clean and was purchased out of state. It is for emergencies when I need to make a sensitive purchase. If not used within a year, I transition it up to the 01 slot in order to prevent expiration, and replace it with a new card.

These are just a few ways I have used prepaid cards. It is important to establish your own methods of privacy with which you feel comfortable. Most importantly, know the risks associated with any type of digital payment.

Privacy.com

In simplest terms, this is a service which provides free masked debit cards which charge back to your checking account. A week rarely goes by when I do not use a new or previously created Privacy.com masked debit card. The reason is that these cards are absolutely free to the user. I currently use this service for many scenarios from one-time online purchases to recurring monthly automated charges. The mobile app and web interface make the generation of new cards extremely easy.

At the time of this writing, registration is open, but only to U.S. citizens. As explained previously, Privacy.com generates unique masked debit card numbers that can be used for online purchases without disclosing your real identity to the online vendor. The purchase is passed through to a checking account on file with Privacy.com, and the funds are withdrawn immediately, as is common with any traditional debit card. Due to increasing pressure from the financial industry, Privacy.com must verify all new users. This will require you to provide your real name, physical street address, and date of birth. This data will be used to verify you against public records. If you cannot be verified, you will not get an account. This is frustrating to privacy seekers, but we understand the necessity due to rampant fraud and federal laws.

The resistance I hear from most people is in reference to the requirement to connect a valid bank account to Privacy.com. Who is to say that they will not be hacked? I agree that Privacy.com is now the weak link for a cyber-attack toward your account. However, the same could be said about your bank where you hold the checking account. In my experience, your bank is more likely to get hacked than your account at a masking service such as Privacy.com. Therefore, I proceed with connecting a checking account to Privacy.com. However, I do not blindly attach my primary accounts to this service. Instead, I strategically connect a dedicated account that cannot withdraw funds from any other personal or business accounts. This can be done in a couple of different ways.

Many financial institutions, whether traditional banks or credit unions, issue a primary checking or savings account to each member. Secondary accounts can be added under the umbrella of this primary account. These could be checking accounts to isolate proceeds from a home business or savings accounts to encourage various savings goals. While these are all openly connected to the primary account, they each have their own unique account number. A creation of a secondary checking account and connection of that account number to Privacy.com protects any assets that exist in any other accounts connected to the primary. This provides a layer of protection for those concerned about exposing their finances to fraudulent purchases.

Another option is to create a business checking account solely for use with Privacy.com. The negative result with this method is the likelihood of expensive fees attached to a business

checking account. I have found that in each of these scenarios, there is usually a minimum balance that can be maintained to avoid any checking fees. I keep these accounts funded at all times in order to meet the minimum requirement, but not enough to cause a panic if fraud wiped out the account. Everyone's threshold for this will vary.

The best feature of Privacy.com is the flexibility in setting up each card based on what it will be used for. By default, cards are designated as "Merchant" or "Burner" cards. Merchant cards will attach themselves to a merchant (the first merchant to place a charge on the card). Once this has happened the card cannot be debited by any other merchant. Burner cards are single-use and expire after the first charge has been placed on them. These cards should be used for different purposes.

Merchant cards should be used for recurring payments. Since there is no charge for Privacy.com cards, you can create cards and leave them active indefinitely. Attaching to a single merchant is a huge security benefit. If the merchant spills customers' credit card data it will not affect you at all, because the original merchant is the only one who can debit the card. When creating a Merchant card, you can define a maximum transaction limit per week, per month, per year, or per charge. There are reasons to use each of these options. For example, when setting up a utility bill that will be charged monthly, you can use the "per month" option, limiting the total charge amount to what your maximum electricity bill might be. For items like auto insurance which are only billed annually or semi-annually, you may wish to use a yearly or per-charge total instead, setting the limit to your annual insurance rate.

Another important feature of Privacy.com Merchant cards is the ability to "pause" the cards. This allows you to ensure that the card cannot be used unless you log in to Privacy.com and re-enable it by clicking the "Play" button. This is a great feature for cards that are used infrequently on services like online retailers. For instance, you may wish to have an Amazon account, but you might not want the card to always be active if you only use it occasionally. This allows you to freeze the card, ensuring nothing can be billed to it by any merchant without your consent.

If desired, you can also associate multiple bank accounts to your Privacy.com account. This is useful if you have several accounts whose transactions you would like to protect with Privacy.com. All of the settings applied to Merchant cards can be changed at any time, with the exception of the merchant. Once the card has "locked" to a merchant there is no way to reverse this. I believe this is a highly desirable feature, as it prevents users from re-using the same credit card number on multiple sites.

Burner cards are only valid for a single transaction. The use-case for these cards is different than that of Merchant cards. Burner cards should be used for one-off purchases from merchants which you don't fully trust; will not use again in the future; or who are likely to

implement recurring charges after your initial transaction. As soon as the initial charge is debited from the card, it expires and can never be used again.

When using Privacy.com cards, you can assign any name you like to the card. You can also use any billing or shipping address you like. There are many ways you can use this flexibility. You can use it to order packages to your home without revealing your true name. In this case, you would use the alias name of your choice and your home address as both the shipping and billing address. You can also use it to create disinformation by giving your real name and a false billing address when purchasing online services which do not need shipped to a home. You are limited only by your imagination.

The final customization I like to make to any Privacy.com account is to enable "Private Payments". This feature is disabled by default. When you make a purchase to Amazon through a virtual Privacy.com debit card number, the transaction on your bank statement appears similar to "Amazon - $54.03" or "Privacy.com-Amazon". This discloses the merchant to your bank which provides your checking account. Your bank still knows everywhere you spend money. The "Private Payments" option in Privacy.com allows you to choose one of the following entities which will be displayed for all Privacy.com purchases.

Privacy.com
H&H Hardware
Smileys Corner Store
NSA Gift Shop

While the NSA Gift Shop entry was an option which I jokingly proposed to the CEO of Privacy.com when he was on my podcast, I do not ever use it. I usually choose the Privacy.com option for all clients. This way, all uses of a masked debit card will appear as Privacy.com on the bank statements. Since the bank already knows the source of the transactions, I do not find this reckless. It will remind the client that the charge originated from their Privacy.com account. More important, the bank will not know the identity of the actual merchant for each transaction. If an adversary is in possession of a subpoena for your bank records, or has obtained unauthorized access to your bank account, no information will reveal the details of your purchases.

In 2019, I contacted an old friend who now works at a branch of the bank I use for business purchases. I asked her if I could see the details of some transactions on my account, and she obliged. I brought in my statement which displayed only "Privacy.com" and the amount of purchase on three specific transactions. She turned her computer screen toward me, and showed me the full record of the first transaction. It displayed the following details (with my explanations in parentheses).

- Date of transaction (The date which matched my own records)
- Amount of transaction (The amount which matched my own records)
- Privacy.com (The merchant which matched my own records)
- Privacy.com PRIVACYCOM (If I had not chosen to hide the merchant, it would display the merchant name first, such as "Amazon.com PRIVACYCOM")
- ACH Trace # (844) 771-8229 (The telephone number for Privacy.com)

In other words, the detailed records at the bank did not identify the merchant, such as Amazon, for each transaction. A court order to Privacy.com would obviously reveal this, but partner companies of my bank, and entities such as Early Warning, do not get to see the data.

As with any important accounts, be sure to choose a very strong username and password for your Privacy.com credentials, and enable two-factor authentication through a software token such as Authy. I also encourage clients to "close" cards which are no longer needed. This action permanently closes the cards, and allows you to make new cards for similar purchases. Some users have reported that multiple open cards for the same merchant, such as Amazon, flags the account as suspicious and may cause an interruption. While I have not been able to replicate this, it makes sense to close cards as soon as they are no longer needed.

Privacy.com Concerns

It would be false to say this service was a perfect privacy solution. Any financial institution is bound by government requirements to track and verify users, and Privacy.com is not immune to these demands. This service relies on a third-party company called Plaid in order to verify user identities and monitor transactions. We do not know the depth of involvement Plaid has with Privacy.com, but we know there is an exclusive relationship between the two. Since Plaid connects to thousands of banks and is primarily funded by companies such as Goldman Sachs, American Express, and Citibank, I assume that various levels of data sharing exist. This is not a pleasant thought, but the best option we have for free virtual debit cards.

What does this mean in the real world? I believe that transactions through Privacy.com provide value to us. They allow us to use alias names and prevent merchants from knowing our true identity and account details. It helps us prevent credit card fraud and unauthorized card transactions. It is NOT a mechanism to hide transactions from banks, governments, or credit agencies. I believe the anonymization protections stop immediately after the merchant. It is important to understand these limitations and not assume this service is a magic solution. While I rely on Privacy.com card numbers every day on behalf of myself and clients, it can never replace the anonymity provided by cash.

Trust / LLC Checks

If you established bank accounts in the name of your trust or LLC, you may wish to have checks available for semi-private payments. If you need to write a check for a product or service, one from a trust account without your name may provide more privacy than a personal check containing your name and address. When you open the bank account, most institutions will give you some free temporary checks. These are designed to provide immediate payment options while you wait for a full order of checks to arrive. If you decide to go this route, please consider the following.

The bank will usually offer five to ten free checks. They print them on-site on professional paper stock. I like these because they are usually the larger sized version which appear more professional than a smaller personal check. I always push the limits here and ask for double the amount offered. On one occasion, I encountered a new employee who was instructed to do anything to make the customer happy. I walked out with 150 "temporary" free checks. These checks do not expire, and you may never need to order more.

The bank will likely place all known details on the checks. This often includes the LLC or trust name, your name, your address, and your role in the entity. This eliminates any sense of privacy. I always ask that only the name of the trust or LLC appear on the check. If questioned, I advise that I might be moving soon and would rather not provide an inaccurate address. Most importantly, I do not want my name listed on the check. Most banks comply with this request.

If you need additional checks, I do not recommend ordering through your bank or any third-party services. Regardless of your directions to the bank, it will still likely place your name and address on the checks. Third-party check printing services are more demanding. Due to fraud and abuse, most now require you to include a name and physical address which can be verified through public records. They will only send the checks to the address printed on them.

I prefer to print my own checks. This may seem shady, but it is completely legal. I purchase professional check paper through Amazon and create an Excel spreadsheet for easy printing. I can now print my trust name with routing and account numbers at the same time I enter details about the payee on the check. I can choose whether to include any address I like, such as my PMB or UPS box. Usually, I do not include any address. Printing your own checks allows you the freedom to control the data disclosed within each. As long as you are providing accurate entity titles and account details, there is no fraud here. Overall, I possess checking accounts for most of my trusts and a few of my LLCs. I will later specify the few instances when this format of payment is preferred over other options.

Secondary Credit Cards

Most credit card companies will issue additional cards at your request. These cards usually possess the same account number as the primary card and all charges will be applied to the primary account holder. These cards are often requested by parents to give to their children for emergencies or by individuals to allow usage by a spouse. Any time the secondary card is used, the charge is processed as if the original card had made the purchase. Since the secondary card is part of an account that has already been confirmed, there is usually no verification process to obtain the additional cards.

To request an additional card, which you should refer to as "Secondary" or "Authorized User" cards, you should contact the credit card company by calling the telephone number on the back of the card. Tell them that you want a duplicate card in the name of a family member. You can request an additional card in any name that you want, including your new alias. You will be warned by the credit company that you are responsible for any charges, and the new card will be sent out immediately to the address on file for the account. If you do not want this new name associated with your home address, be sure to update your address on file with the credit company to your PMB or UPS box as previously explained. I recommend confirming that the new address is active before ordering additional cards.

Many readers of previous books reported difficulty in obtaining a secondary card from traditional banks, such as Bank of America or US Bank. Readers report that these entities demand a DOB and SSN for each secondary card holder. I have found this technique to work best with traditional credit card companies, and it has never worked for me with a debit card. In a moment, I present my updated recommendation for secondary cards since the previous edition of this book.

You may be reading this and thinking that there is no way that this could be legal. It is absolutely legal as long as you are not using this method to commit fraud. The card is attached to your account, and you are paying the bill. It is not identity theft because you are not claiming to be a specific person. If you were using someone else's Social Security Number and opening credit lines with their information, then this would be illegal. You must only apply this to your own account over which you have authority. Additionally, you must always follow the rules.

- Never provide your alternative name to law enforcement or government officials.
- Never open new credit lines with your alternative name.
- Never generate any income with your alternative name.
- Never associate any Social Security Number with your alternative name.
- Never receive any government or community benefits in your alternative name.
- Only use this name to protect your privacy in scenarios with a credit card.

Secondary Credit Card Concerns

There is a fine line between the use of an isolated alias name and possessing a secondary credit card in that name. If an alias name is needed due to death threats, you should never obtain a secondary card in this new name. This is because the credit card company associates you to the alias and reports this information to numerous third-party organizations. Consider the following scenario which represents my own unfortunate experience with Chase.

I possessed a Chase credit card in my true name, associated with my SSN. During the application process, I requested a secondary card in an alias name. For my own privacy, I will not disclose the name. Assume it was "Mike Doe". I never used the card which was issued in my true name. I only wanted the account for the secondary card in my travel alias name. This way, I had a credit card in an alias name when I checked into hotels under that alias. Since I had never used that card in my true name, I should have some isolation between me and my alias. This is actually quite incorrect.

A few months after I began using the secondary card, I conducted a query of my own name within the data aggregation service CLEAR. My report immediately identified "Mike Doe" as one of my associates and aliases. This is because Chase shares the details of every card holder with dozens of other companies. Per their online privacy policy, Chase shares full details of your account and transactions for "joint marketing with other financial companies" and their "affiliates' everyday business purposes". In other words, Chase tells others what you are doing. Furthermore, Chase does not allow you to limit or prohibit this sharing. While all credit cards share some data about your transactions, Chase seems to go overboard. Because of this, I have canceled all of my Chase cards and I no longer recommend them to clients. In a moment, I explain my current process.

Secondary cards have caused much confusion with my clients. I present two scenarios which may help identify when it is appropriate to use a secondary card and when it should be avoided.

- I possess an alias name which I use while I travel. I check into hotels under this name and I possess a secondary credit card in the name. It is loosely associated to me through financial records, but not within public people search websites. It allows me some privacy while outside my home but a non-public digital trail exists.
- I possess an alias name which is extremely confidential. It is only used in situations where I do not want to be associated with my true identity. It has been used during the purchase of my VPN, cellular telephone, and mobile data plan. I would never obtain a secondary card in this name. It would create a trail from me to the services and devices for which I want to remain private.

Current Secondary Credit Card Protocol

I have possessed secondary credit cards in various alias names for over a decade, and I have helped countless clients replicate their own process. In 2020, I substantially changed my credit card protocol for clients. As stated previously, I no longer recommend Chase cards, and now encourage clients to obtain American Express (AMEX) accounts. Part of this is because all Chase transactions are captured by both Visa and Chase, and both refuse to allow you to control sharing of the data. Chase's online privacy policy also clearly boasts that you cannot limit data sharing to third parties. Let's compare that to American Express.

If you log in to an active AMEX account and navigate to Account Services > Security & Privacy > Privacy Preferences, you will see similar third-party sharing options which were present with Chase. However, AMEX allows you to disable all of them, which I recommend doing. In fact, AMEX was the only card I could find which allowed the consumer to prohibit sharing to outside companies. Furthermore, since AMEX is not affiliated with Visa or MasterCard, you are eliminating additional exposure by keeping these purchases within the AMEX network. However, there is one more area to adjust. Navigate to the following direct website and disable "Information Sharing" on any card presented.

https://online.americanexpress.com/occ/auth_inquirepiisharing.do

After these modifications, I believe you possess the most private credit card option available today. No credit or debit card is anonymous, and all leave a digital payment trail. Since daily credit card use is required by most of my clients, I simply try to find the lesser of all evils.

AMEX encourages additional authorized user cards for both personal and business accounts. You can submit a request online or via telephone. However, AMEX demands an SSN and DOB be attached to every secondary credit card issued. This presents a big problem if you want a card for "John Doe" but do not have a valid SSN to provide which matches that name. Instead, consider a new strategy. For most clients, a secondary card with only their first and middle names works fairly well as an alias. Assume your full name is George Michael Bluth. Using George Bluth, Michael Bluth, or the full name could be a privacy invasion, especially when checking into a hotel. However, George Michael is generic. It is also not a lie. Many clients have expressed concerns about using a completely fake alias, especially those carrying security clearances. Using only a first and middle name is usually much more acceptable.

I typically tell a client to call AMEX and ask for a secondary card be issued in only the first and middle name. Explain that you are the victim of stalking, and prefer not to use your last name at hotels. Advise the AMEX personnel to add your own SSN to this card. The new card will not have your last name displayed. I believe there is a much clearer legal use of an alias card which displays true information than one which is completely fake.

For extreme clients, I still rely on completely alias-named cards through AMEX business accounts. Although AMEX encourages users to add an SSN and DOB for each cardholder, the business accounts allow more discretion, and they will issue cards to any name desired without providing an SSN when pushed. Recently, the following steps were used with a client.

- Generate an EIN from the IRS for your LLC. If you do not have an LLC, register for an EIN as a sole proprietor. AMEX may scrutinize sole proprietors for business cards.
- Apply for a free AMEX business card with true name, SSN, and EIN via telephone. During the process, request a secondary card for an employee. When prompted for a DOB and SSN, consider a response similar to, "Our company privacy policy prohibits distribution of employees' SSNs. I accept all responsibility for the usage of the card and authorize my own SSN to be used."
- Provide one or multiple alias names for the new "employee cards".

I have helped clients obtain business cards as sole proprietors without the need for an LLC on numerous occasions, but having the LLC EIN provides a much smoother process. One client possesses a business account with over 20 alias cards without ever providing any additional SSNs. The limit imposed by AMEX is 99 cards, but I never recommend testing this. Finally, I present what I believe is the best feature of the AMEX secondary business cards: each card possesses a unique number. While the numbers are very similar, the last five digits are unique. Consider the following reasons why this is important.

- A retail business does not know that your alias card is under the same account as your personal name. If you had used your real Chase credit card at a grocery store and later switched to using the alias Chase card, the store knows the same number is on each and treats the purchase history as one. AMEX cards are not vulnerable to this.
- Many online retailers restrict credit card numbers to a single account. If you have a credit card number within an account in your true name, creating an alias account with the same number will cause issues.
- Companies which share purchase information with third parties will not be able to disclose that your personal card number is associated with your alias card.
- Hotels cannot associate your previous true name with your new alias by comparing credit card numbers used during payment.

AMEX is far from perfect. It is still a credit card company profiting from your activity. Compared to traditional Visa and MasterCard providers, I believe AMEX is a much better choice for both privacy and alias usage. Be aware that AMEX conducts a soft pull on your credit each time you request a secondary card, and will require a credit freeze to be lifted each time you add a card. I always recommend applying for any desired secondary cards at the time of application in order to avoid these roadblocks.

Alternative Secondary Credit Card Protocol

There are three concerns from some clients in regard to AMEX credit cards. The first is that AMEX typically requires a slightly higher credit score than most Visa providers in order to be approved for an account. The second is the occasional merchant which does not accept anything other than Visa or MasterCard. Finally, some clients do not want the awkward telephone call with AMEX support during which they must convince the representative to create a secondary card in one name while associated to the SSN of the account holder. Most clients want a simple option for numerous secondary alias credit cards without much resistance from the provider. In these scenarios, I recommend Capital One credit cards.

First, I should note that Capital One has a privacy policy almost identical to Chase. You cannot control the major data-sharing abuses. If you choose a traditional credit card such as these, I believe it is vital to be using a PMB or other CMRA address as the physical "home" address. They will absolutely share account details with data mining companies and credit bureaus. I do not possess a Capital One card, but I recently helped a client obtain an alias card via a brief phone call. After calling the number on the back of the primary card, we explained that we wished to obtain two "Authorized User" cards, per the following wording on Capital One's website.

"An authorized user is someone you add to your account without any additional application or credit check. They'll get a card with their name on it and share your line of credit. As the primary cardholder, you'll still be responsible for all charges and, if you have a rewards card, you'll earn on every dollar they spend."

The representative only asked for the names desired on the cards. After reading a warning about the primary card holder being responsible for all purchases, the cards were shipped. In three days, my client possessed two credit cards in alias names ready for use. Both cards displayed the exact same card numbers as the primary card in her real name. This is a minor issue, but we should all be aware of the risks when using multiple names with the same card number. If the primary card in the real name is never used, this is not much of an issue.

Obtaining secondary cards through Capital One was much easier than AMEX. However, privacy is not always easy. I believe it is worth the effort to secure AMEX cards in alias names with unique card numbers. This helps hide your true identity from merchants. If AMEX is not an ideal option for you, I prefer alias Capital One cards over any card in a true name. You must choose the level of privacy (and effort) desired and then execute your strategy. Expect failure at some point, and then keep pushing until you achieve the level appropriate for your needs.

Secured Credit Cards

I have not found a credit card provider which would agree to provide an alias card in the name of only a trust or LLC. This is unfortunate as such a card would not include any name at all, eliminating the need to use an alias. Traditional business credit cards require your SSN and a full credit check, and they will still place your name on the card above the trust or LLC name. My only solution to this is to obtain a secured business credit card. Secured business cards allow business owners to set their own spending limits by placing a refundable security deposit that doubles as their credit line. The security deposit is important because it protects issuers from the possibility of default which thereby allows you to qualify for most secured business credit cards regardless of your credit history or how much disposable income you have. For our purposes, a secured credit card replicates a prepaid card, but has a much more professional appearance.

These cards can display a business name, including a trust or LLC, without the need for a real name underneath. There are two main types of secured cards. The first, and most popular is the type that builds a line of credit for the business while it is used. We do not need that. Instead, I search for cards that simply provide a limit equal to the current balance of the account. I also look for cards that do not require an SSN. These will demand an EIN for your business, so these will be limited to LLCs only. If you want a card issued in the name of your trust, you will need to contact numerous companies. Be prepared to be declined, but I occasionally find a new secured card that is less restrictive. The following online searches may be of great benefit.

secured credit card no ssn
secured credit card no ein
secured credit card ein only

Recently, I have found a few physical banks which offer secured business credit cards. If you have already established a personal account at an institution that offers these, it will be much easier to customize your card. I recently entered a bank branch where I possess a personal checking account. I advised that I had created a new LLC, and wanted to obtain a secured credit card. I stated I was not looking to establish credit, and only wanted the card for convenience. I deposited $1,000 into a new account and received a card with only my LLC name visible within a week. I can now use this card without disclosing my name.

Now that we have your sources of payment established, we need strategies on the proper use of each. There will be many times over the first few months of residency in a new home when a service or utility needs to be activated. You will be asked for your full legal name, address, DOB, SSN, and other sensitive information. None of your personal details should ever be associated with your home address. We will need to be creative and resourceful.

Alias Wallets

Isolating your aliases within their own wallets is vital for my clients. You do not want to keep secondary credit cards in alias names in the same location. Presenting a credit card in one name while you are holding two additional cards in other names looks suspicious. You want to be able to immediately access any credit cards or non-government identification cards as if it were natural. While I can offer a couple of ideas, you should ultimately choose the method best for you. Hopefully the following will generate your own thoughts.

One of my clients carries four "slim" card wallets. These are small, thin wallets which hold a couple of cards on each side with a thin pocket in the middle for cash. He chose RFID-blocking wallets, which is also my preference. These are abundant on Amazon, but I currently only use the Silent Pocket options. These are available in several colors, and the following is the strategy he and I found best for his needs.

- **Blue**: This wallet is associated with his true identity containing his real driver's license, passport card (no address) and credit cards. He chose blue for this one as it is the wallet he will retrieve when stopped by the police for his awful driving (blue lights). The passport card can be used when an official ID is needed, but he does not want to share a home address (PMB).
- **Black**: This wallet is his primary alias that he uses for travel purposes. This contains a secondary credit card in his alias name which he uses for hotels, dining, and social interactions. It also contains his alias gym membership card, "employer" ID, and random travel reward cards. They are all in the primary alias name.
- **Green**: This wallet is designated only for shopping (green reminds him of money). It possesses prepaid credit cards and gift cards. No identification is required. He grabs this whenever he will be purchasing anything from a physical store.
- **Red**: The final wallet is red and only used during international travel. It is the larger style of passport wallet. It contains his passport, official state ID in his real name, and a second credit card in his real name reserved for international use. It is the primary form of payment for this wallet. Each of these four wallets contain a few hundred dollars in cash for emergencies.

Another client chooses to use binder clips as his wallets. His situation is very unique and he possesses four "wallets" at all times. Each set contains the appropriate identification cards and secondary credit cards, with a small amount of cash folded once around the cards. The small binder clip holds it all together. He knows immediately which alias is represented by the type of currency on the outer layer of the wallet. The $20 bill is the primary, the $10 bill is the secondary, the $5 bill surrounds the third alias option, and a $2 bill covers the fourth.

ID Scanning and Copying

Chapter Six briefly discussed optional responses when a car dealership demands to copy your license when purchasing a vehicle. I want to revisit this under new context. We now see many retail establishments demanding to store scanned copies of identification or collect text details of IDs from various barcodes stored on the backs. This is usually unnecessary and the data collected is often abused. I have witnessed the following scenarios within one month while updating this chapter.

Retail Returns: Due to an abundance of gift card fraud, retail establishments have cracked down of returns of products. Stores such as Walmart and Target are members of an entity called Retail Equation. This company monitors returns to retail stores. When the store requires identification in order to return a product, they typically scan the ID card and the details are sent to Retail Equation. If your passport card does not populate the desired fields, the employee will likely manually enter your details. All of your returns are stored and analyzed. If you return enough products to trigger a flag on your account, stores will stop accepting returned items. Your profile is available to many companies and other unknown recipients.

Medical Organizations: Any visit to a doctor, dentist, hospital, or urgent care is going to require identification. I accept this, as they need to verify insurance benefits and ensure proper prescription details are transmitted. However, I do not allow anyone to collect a digital scan of my photo within any identification card.

Pharmacies: I recently required a prescription eye drop. It was not a controlled substance, and not a medication which is abused. However, the pharmacy demanded I present valid ID. After displaying my Passport card through a windowed wallet, they demanded I remove the card so they could scan it into their system. The scan was a digital acquisition which would populate my details and store my photo forever across their nationwide network. No thanks.

Entertainment Establishments: In late 2019, I went out with friends to a comedy show in Los Angeles. After submitting my ticket for entry and displaying my passport card to prove I was of legal drinking age, I was told they needed to scan my ID into their system. When I asked where the data was stored, the level of encryption applied to the transmission, and to see a copy of the terms of service for this requirement, I was told to move along.

Adult Products: If you have ever purchased alcohol, you have likely been "carded". Many years ago, this meant flashing my ID and the clerk doing the math to make sure I was of age. Today, stores require the clerk to scan the barcode on the back in order for their systems to determine that my date of birth is valid for purchase. Many of these systems record the details and share them with third parties.

My solution to this is two-fold. First, I only provide a U.S. Passport card whenever an entity wants to scan a barcode stored within an identification card, such as a grocery store. This is because the barcode on the back of a Passport card simply contains the numeric digits directly to the right of it, which only identifies your card number. There are no personal details stored within this code. Furthermore, most businesses, such as grocery stores, do not have software which knows what to do with these details. The card number obtained during the scan will likely get rejected. Most scanning systems are looking for a date of birth, name, and address. All of these details are present within the barcode of most driver's licenses or state identification cards. Second, I rely heavily on the federal law mentioned earlier. U.S. Code, Title 18, Part I, Chapter 33, Section 701 states the following.

"Whoever manufactures, sells, or possesses any badge, identification card, or other insignia, of the design prescribed by the head of any department or agency of the United States for use by any officer or employee thereof, or any colorable imitation thereof, or photographs, prints, or in any other manner makes or executes any engraving, photograph, print, or impression in the likeness of any such badge, identification card, or other insignia, or any colorable imitation thereof, except as authorized under regulations made pursuant to law, shall be fined under this title or imprisoned not more than six months, or both."

This law was created for military identification cards and insignias, and was likely never intended for our use. I have this exact wording, followed by a URL which can be used to verify the content (https://www.law.cornell.edu/uscode/text/18/701), printed onto a sticker and affixed to the back page of my passport. When I use my Passport as identification during one of the previous scenarios, such as a visit to a doctor, and an employee insists on copying the identification page, I present this section of my passport. I explain that I could be committing a crime allowing the passport to be photocopied. If needed, I sell it further by telling the employee that he or she may definitely be committing a crime by doing so. It is always met with skepticism, but most employees do not want to take a chance with federal law. I always offer them the URL so that their manager can look up the law and see if they agree. Most do not indulge me, and move on to the next requirement of my visit.

Whenever you make purchases using the techniques throughout this book, you are likely to be asked for identification. I hope that you consider these solutions when this happens. I have encountered numerous data breaches which included full digital scans of passports and identification cards. I do not want to ever be exposed within these common occurrences, and I suspect you feel the same way. The more of us who refuse this unnecessary privacy invasion, the more common our rebelliousness becomes. It may create awareness for future visits. When all else fails, and an employee demands to copy my ID, I respond "Of course! However, I would like a copy of yours first. Is that acceptable by you? If not, why?". I have yet to experience an employee allowing me to copy their ID, as that would be a privacy invasion.

Home Insurance

Acquisition of any type of insurance always brings difficulties when attempting to achieve privacy. Insurance companies want to know whom they are protecting. They will use your credit score to determine their risk providing you coverage. Misrepresenting yourself or your entity is not only illegal, it will likely eliminate any payout when you need to file a claim. Imagine you provided an alias name to the insurance provider and your home was destroyed. You file a claim, which is approved. The check is written to your alias. How would you deposit it? What if you are required to display identification to receive the check? What happens when a neighbor sues you because of a fall on your property? Your insurance company will not cover you if your name is not on the policy. These are real issues.

The bottom line here is that your home insurance policy will need to be accurate. This does not mean that you must give up all personal privacy. You have a few strategies at your disposal which can provide various layers of privacy while remaining legal and properly protected. Before I discuss my recommendations, I present past experiences that should be avoided.

In 2018, I assisted with the purchase of an estate. My client wanted to remain completely anonymous and was quite wealthy. The purchase of the estate with cash was simple, and the utilities were all activated with alias names or details of the trust. The last issue was insurance. All providers in that area demanded to know the name, DOB, and SSN of the home owner and account holder. The trust could be named as a secondary insured party, but the policy mandated full details of the owner. The insurance companies confirmed that any payment made due to a claim would be paid to this name, and not the trust. There was no budging. Either my client disclosed his true identity, or there would be no policy.

My client chose the latter. He decided to simply avoid home insurance altogether. He was wealthy, could have purchased numerous additional homes in cash, and decided that his privacy was worth more than the money he could lose after a catastrophic event. I discouraged him from this, but his mind was made up. To this day, he possesses no home insurance coverage.

I disagree with this decision for two reasons. First, a home is likely our biggest asset. If a tornado or fire destroys the home of my clients, they are unable to purchase another. If they possess a loan on the home, insurance is mandatory. Economically, it does not make sense to proceed without insurance. Additionally, you now possess great personal liability. If someone is injured on your property, you are the sole party reliable for payment. This could quickly bankrupt you. Therefore, I insist on insurance for my home, and I strongly encourage my clients to do the same.

Some may wonder why we can't use our trustee for the insurance policy. We could, but this is probably a very bad idea. Your trustee would need to provide their own personal details, and the policy would be priced based on their credit history. Next, this would likely violate the terms of the policy. Almost every home insurance policy states that the listed party must be an occupant of the house. The fine print will usually specify that immediate relatives also possess coverage. Technically, you might be covered if your sibling was your trustee, but I think you are playing with fire.

The following methods assume that you established a private home titled to the name of your trust. Whether you possess a loan or paid in cash will not matter. These tactics attempt to obtain completely legal and appropriate coverage for your home.

My first recommendation is a personal visit to a handful of local providers in the area of your home. Calling random online providers will get you nowhere. They will not provide a quote or any details without the immediate demand for your name, DOB, and SSN. These are all out for me. I call ahead and ask to arrange a meeting to speak directly to the local insurance agent for each business. I ask to reserve the meeting under the name of the trust. If I am pushed for a real name, I advise that I am not sure which trustee will be at the meeting. I show up in person, well dressed and polite.

I start with some honesty. I advise the agent that I represent a trust which is in the process of purchasing a home. The occupant(s) of this home are very private. They have been the victims of stolen identity, cyber-crimes, and other unfortunate situations. I further explain that the full details of their identity, including DOB and SSN have been publicly exposed. This likely applies to every American citizen. If appropriate, I conclude that one of the occupants has been harassed and threatened, and is in fear of a physical attack. I explain that I am taking every step I can to ensure that their true identities are not publicized on the internet.

At this point, I rarely receive any resistance. I usually see signs of empathy on the face of the person with whom I am speaking, and all of these scenarios seem very common. I proceed to ask some very detailed questions. I already know the answers, but I find that allowing the agent to discuss the situation creates a better dialogue.

What information will you need about the owner of the home?
Can the policy be placed in the name of the trust?
If not, can the trust be listed as a secondary insured?
Does your parent insurance company share customer data with any third parties?

In almost every discussion I have had in these scenarios, I learn the following:

- Almost every insurance provider allows the inclusion of the trust name as a secondary insured party, but rarely as the primary policy entity. This applies to traditional home policies. A Social Security Number will be required to generate a new policy.
- Insurance companies insist they never share customer details with third parties. Minimal online investigation reveals this to be inaccurate. As only one example, consider the privacy policy of State Farm. It begins with "We do not sell customer information". The excerpts below identify the ways in which they share customer details. The content in parentheses is my own opinion of how this could expose your home address.

"We share customer information inside or outside our family of companies":

- for our everyday business purposes, for public policy purposes, and as permitted or required by law. (This is a catch-all, and gives them the right to do practically anything they desire with your information.)
- as needed, to handle your claim. For example, we may share name, address, and coverage information with an auto body shop to speed up repairs on auto damage claims. (This allows them to share your true name and address with any service provider. This eliminates the idea of using an alias name for the company that will replace your porch after a storm.)
- with consumer reporting agencies, for example, during the underwriting process. (This is the most invasive. These agencies devour your personal information, and amend your profile. You will not be anonymous very long.)
- in connection with a proposed or actual sale, merger, transfer, or exchange of all or a portion of our business or operating unit. (If this insurance provider is sold to another company, your information is transferred and the new privacy policy applies.)
- with companies that perform marketing or other services for us or with whom we have joint marketing agreements. These agreements allow us to provide a broader selection of insurance and financial products to you. (This basically allows the insurance company to share your details with any company willing to purchase it.)

The summary here is that every major insurance company has the right to do whatever they want with your information and it will be exposed at some point. Therefore, we must take our own precautions. Now that you know the risks, let's establish our best defense possible.

In 2017, I assisted a client with the purchase of an anonymous home. She was the victim of a targeted home invasion, and sought a safe place where she could not easily be found. Home insurance should be secured before the closing date, as you should have protection the

moment you own the property. I visited a major insurance chain that possessed a local office and an independent agent. We made it through the small talk and I explained the unique scenario of my client. He seemed very willing to assist any way he could.

My first concern was the issue with the trust. I explained that my client, and the true occupant of the home, was not the trustee of the trust which is purchasing the property. Therefore, lumping together the entire policy into one entity might not make the most sense. I asked if he could provide a business policy in the name of the trust and a separate renter's policy in the name of my client. This is common with rental homes and other situations where a business entity owns the property but does not reside in it.

With a traditional home insurance policy, there is coverage of the dwelling, property, and liability. There is also protection for the contents. This is a typical "package deal". If you owned a rental property, you would want protection if the house was destroyed or someone was hurt. However, you would have no interest in coverage for personal items, such as the renter's furniture. These policies are more affordable because they provide less protection than a traditional policy. If your tenant wanted coverage, he or she could purchase a renter's policy to cover only their belongings. I like to apply the best of both worlds toward my clients' policies.

I explained that I desired a policy in the name of the trust as a business entity for the home and property. The trust obviously will not be an occupant. The trust would own the policy and make payments. The trust is covered from a liability perspective and the property is covered from damages. This type of policy is commonly used for businesses. Since no business will be conducted, and the property is not open to the public, the fees associated with this type of policy are usually quite affordable.

For my client, I requested a renter's policy in her name. This covers her possessions inside the home. One way to explain it is that the policy would cover anything which fell out of the house if you were to pick it up and shake it. The business policy protects everything else including liability. These policies are very affordable, as there is a much less likely risk of a claim.

The reason I want to do this is because it allows me to have the home policy purely in the name of the trust. While the renter's policy will be in the name of my client, I have a bit more control over the information stored in that account. The provider will obviously know that my client lives in this home. However, I can place the address of a UPS box as the primary contact for the renter's policy. If the details of this policy are shared, sold, or lost, the associated address will likely be the UPS box. While a business account can also possess a UPS box for billing, there are many references to the real property address all throughout the policy.

You may recall that I previously wrote that an SSN must be associated with the policy. This is absolutely true. Since I am purchasing the renter's policy through this office, and supplying a full name, DOB, and SSN of my client, the office now knows the true identity. The "soft pull" credit check for the renter's policy can be used to pacify the requirements for the trust policy. As the grantor of the trust, my client has a direct nexus, even if she is not the trustee.

As an extra layer of privacy, I proposed an additional request. I explained that my client is considering returning to her maiden name. I requested that the renter's policy be placed into this maiden name now, even though it is associated with her true DOB and SSN. The company will know her true name through the credit check, but the policy and annual bill will be in the maiden name. This isn't going to fool an advanced private investigator, but it will make her a bit more difficult to find in the wake of a large data breach. Let's summarize the coverage.

My client possesses a trust. She is the grantor but not the trustee. The property is protected with a business policy in the name of the trust. It covers the home, land, and liability of both. My client's name is not listed anywhere in this policy, and the trustee digitally signs the official policy, executing it at the time of closing. This annual bill is paid with a designated Privacy.com debit card, which is connected to the trust's checking account.

My client possesses a separate renter's policy which is in her real maiden name and SSN. It covers her belongings inside the home. The address for the policy and billing is her UPS box. The policy contents include the real address, which is not public record. This bill is automatically paid through a second Privacy.com debit card, connected to her personal checking account.

Is this bullet-proof? Not at all. The insurance company is the weak link. They know my client and her home address. This is not optimal, but is the closest we can get to our desired level of privacy. Two years after I executed this plan for my client, I am still unable to locate any official connection between her name and the address of her home. This is the best I can do for her situation. The irony of this scenario is that the combined cost of her trust policy and the renter's coverage is less than the policy quoted as a traditional full coverage home. The business policy even has twice the liability protection. This is mind boggling.

If you do not possess a Privacy.com account, a personal credit card could pay the renter's policy and a check in the name of the trust could pay the home coverage. The formalities of this are not too important, but I like to pay with separate accounts when possible. Your mileage will vary with this. I have presented this proposal to over thirty insurance companies in various states. My success rate is 45%. With enough determination, you can achieve your own success. I insist you be honest with the person with whom you are speaking. A policy is useless if you can't file a claim due to inaccuracies within the application. Allow the local agent to make the policy work for your situation.

Utilities

The next hassle is dealing with the power and natural gas companies. Thanks to fraudsters that rack up large bills and then leave town, you and I must now provide access to our credit profiles in order to establish basic services. The default demands of these companies are to obtain a full name, DOB and SSN. This information will be verified with a consumer agency and attached to your profile. These services will then share this data with additional data mining companies. It is a vicious cycle.

Over the past five years, I have had various levels of success using alias names and sob stories. Many of these techniques no longer work. If I claim I am not an American citizen with an SSN, I am required to send a photocopy of a passport. When I state I am the victim of identity theft, there is no longer any sympathy. When I offer to provide a deposit for services in lieu of an SSN and credit check, I am told this is no longer an option, and I may be required to provide a deposit regardless. With these rules in place, we must be more creative.

Similar to home insurance, I always establish utilities in advance of closing. You never want to be in a rush to turn on the power. You may give in and disclose your real information just to get past the process. I always start with a polite call to the utility company. Since I record all of these conversations (when legal within one-party states), I can provide an exact transcript of a recent attempt for a client.

"Hi. I have a closing date approaching for a home in [CITY]. The property is being purchased by an established trust, and there are not any occupants defined at this point. What are your options for establishing power in the name of a trust?"

This resulted in the expected response. The operator insisted that a DOB and SSN of the resident would need to be provided. If the trust is a registered business with an EIN, this will usually suffice instead of the SSN. None of these situations apply to us, so I continued with the following conversation.

"I see, thank you. I don't know the SSNs of the eventual occupants, and I don't believe the trust has an EIN due to tax filing requirements. The last property we purchased allowed us to place the bill into the trust name as long as we offered either a deposit or enrolled in autopay from a checking account in the name of the trust. Are these possibilities?"

This resulted in a hold time of five minutes while she contacted a supervisor. I had to eventually talk with this supervisor the next day, but it was a productive conversation. The supervisor confirmed that the utility can be opened in the name of the trust with several requirements. The power company would create an account for the trust the day of the call, but services would not be scheduled. The utility profile would need a checking account

attached to it, and it must be enrolled in auto-pay. The checking account must be in the name of the trust. A debit card was not enough. After this was complete, the supervisor could manually approve the account with a small test withdrawal from the account. After this, a date could be provided to switch on the utilities.

I completed all of these requirements without any issue. The supervisor was very kind about the situation, and more relaxed after she could see the checking account within the system. Every month, the bill is paid through this account. The power company does not know the name of my client. They receive their owed fees in a timely matter every month. There is no fraud. They know the generic name of the trust, which will also be on public record as the owner of this property. The trust checking account is not associated with any personal bank accounts. The bank knows that a monthly bill is paid to a specific utility, but does not know the exact address.

There is an obvious financial trail which could be followed with the proper court orders required. Without these court documents, the name and address of my client will not be connected. You should identify your own threat model, and ensure that you choose the most appropriate tactics. The alternative to this, if you do not have a checking account associated with the trust, is to attempt the use of auto-pay to a Privacy.com debit card. I always offer to pay a deposit to set them at ease, which is usually not required.

Paying a large upfront deposit, which is usually the average monthly bill for three months, will often eliminate the requirement of a credit check. The success rate of this method is decreasing. In a recent worst-case scenario, the utility offered to bypass the credit check only if I submitted a deposit of an average year of use. My client had to give them over $2500 in order to stay private. I have had much better success by using a checking account in the name of the trust. I encourage you to identify all of your options before choosing the best route.

Once you have power established, the rest is easy. Often, the water and sewer companies will rely on your registration with the power company to confirm service. I usually recommend establishing auto-pay to a Privacy.com debit card. If there are fees associated with this, or you do not have that option, auto-pay to a checking account in the trust name should pacify their demands.

Overall, I prefer to establish all services in the name of the trust. Since some utilities are loosely connected to the city government, use of false aliases could approach criminal behavior. With a proper trust in place, you might not need any aliases. When electronic documents require signing, your trustee has the legal authority to comply. When these companies release your billing details privately and publicly, there will be minimal damage. The trust is already publicly connected to the property.

Internet Service

I believe that the most important utility or service which you can anonymize is your home internet connection. Possessing internet service at your home address in your real name jeopardizes your privacy on multiple levels. Many providers use their subscriber list for marketing and it often ends up in the hands of other companies. This will eventually make your home address public on the internet as associated with you. This is possible with any utility or service that is attached to your home address. However, your home internet account shares another layer of your life that you may not realize.

Internet service providers (ISPs) create the connection required for you to have internet access. In its simplest terms, a cable or phone company possesses a very large connection to the entire internet. It creates its own connections to its customers (you). This might be in the form of a cable modem connected to the main connection coming into your house. This allows you to connect to the entire internet through them. Therefore, the ISP can monitor your online activity. Other chapters explain how to mask this traffic with virtual private networks (VPNs) and other technologies. However, you cannot stop the ISP from seeing the amount of traffic that you are sending and receiving, the times of the day that you are online, and details of the devices which you are connecting to their system.

Those who use the technologies previously discussed in this book will likely be protected from the invasive habits of ISPs. However, people make mistakes. You might forget to enable your VPN or it might fail due to a software crash. You might have guests who use your internet without practicing secure browsing habits. Consider the following scenario.

Every day, numerous people receive a dreaded letter from their internet service provider. It states that on a specific date and time, your internet connection was used to download copyrighted digital material. This is usually in the form of movies or music. This practice usually occurs when law firms monitor data such as torrent files which are commonly used to share pirated media. They identify the IP address used for the download, contact the provider of the IP address, and demand to know the subscriber information. The providers often cooperate and share your details. You then receive a notice demanding several thousands of dollars in order to avoid a lawsuit. Not paying could, and often will, result in legal proceedings. There are numerous cases of people who have lost the lawsuit and have been ordered to pay much more than the original asking amount.

I am not encouraging the use of the internet to obtain files which you do not have the authority to possess. I also do not advocate fishing expeditions by greedy lawyers looking to take you down. I see another side of the problem. What if someone uses your Wi-Fi to commit these acts? What if malware or a virus conducts activities which are seen as infringing? I believe one solution to this issue is to simply have an anonymous internet connection. These methods will

only work if you have gone to the extent of residing in an anonymous house as previously explained. If you have not, or are not going to that level, it does not hurt to apply these methods for a small layer of protection. The following is a true example from a client.

My client had recently moved into his new invisible home. He was renting, and nothing was associated with his real name. The electricity and water were included in the rent and associated with the landlord's name. However, there was no internet access included with the rent. My client contacted the telephone company to take advantage of a deal for DSL internet service at a promotional rate of $24.99 per month for two years. He did not need anything faster than this access, and liked the price. He gave an alias name and the real address for the service and was quickly asked for a Social Security Number (SSN), date of birth, and previous address. He tried his best to convince the operator that he would not give this out, and she politely stated that their policy is to conduct a brief credit check before providing access. He gave up and terminated the call. He emailed me asking for guidance. While I had dealt with similar issues for myself and others in the past, it had been a while since I had tested my methods with all of the providers. In exchange for me helping him without any fees, he agreed to share his experiences here.

I first contacted the telephone company offering the DSL connection. Before giving any personal information to the operator, I politely asked about the signup policy and what type of credit check would be conducted. I was told twice that a "soft pull" would be conducted based on the SSN of the customer. This was to ensure that there were no outstanding bills from previous connections and to simply verify the identity of the customer. While telling my sad story of identity thefts, harassment, and threats to my life, I pleaded for a way to obtain service to no avail. Part of the issue here was that a two-year contract was required, and they wanted to be sure that they would get their money. There was nothing to gain here.

I searched for other service providers and found two possibilities. Charter Spectrum cable access and various satellite internet options. Due to speed and cost, I wanted to avoid the satellite option. I contacted Charter and verified the service connection to the residence. They had a high-speed connection of 60 Mbps offered at $59.99 per month. I assured them that I had never had Charter in the past, and asked if there was an introductory price similar to the DSL offer that I had been quoted. As usual, the representative came up with a lower offer. He acknowledged a new customer offer at $39.99 (taxes included) per month for up to one year. I accepted that and knew that my client could likely later negotiate that cost down through threats of canceling when the first year was finished.

I provided my client's address, an alias name that had already been established and associated with a secondary credit card, and requested automatic bill pay through the credit card. I was told that I could set up the automatic payment myself after the account had been established. This was even better. If I were to repeat this process today, I would use an alias name and a

Privacy.com card. This gives my client more isolation from his true credit card account. I got to the end thinking things were too smooth when the personal questions arrived. He needed my SSN in order to complete the process.

I had dealt with Charter in the past and was able to bypass this requirement, so I started testing the situation. I first stated "Oh wow, I was not prepared for that. You see, I was recently the victim of identity theft and the police told me I was not allowed to give out my SSN until the investigation was complete". The operator was very sympathetic and placed me on hold briefly. He then asked for a date of birth in order to conduct the query. I continued to resist and stated "I think that would be the same as giving you my SSN. I will give you my credit card right now, can I just auto pay?". I was then greeted with something I did not expect. The operator stated "The system demands at least a year of birth, can you give me that?". I took a moment to evaluate the risk and provided a year of birth which was not accurate. This seemed odd to me because there is not much the operator could do with that limited information. However, it was enough to get to the next screen. He now needed an email address for the account details and monthly electronic billing. It is always important to have this alias email account ready before any calls are made. He finished the order and the call was terminated.

Three days later, Charter arrived at his house and installed the service. They provided a modem, and charged $29.99 for installation. My client had his secondary credit card ready, but he was never asked for it. Charter conducted the installation, activated the service, and left without collecting any form of payment. The next day he received an email notifying him of a payment due. He created a new account on the Charter website and provided his secondary credit card for the payment (Privacy.com is a better choice today). He then activated automatic payments to that card and enabled the paperless billing option. Today, he continues to receive internet service from Charter and pays his bills automatically through his secondary credit card. Charter does not know his true name. He has committed no fraud. He is a loyal customer and will likely pay Charter for services for the rest of his time at this residence. Charter did not require any contract and he can cancel any time. I was pleasantly surprised.

I thought that this may be a fluke. Maybe I was lucky with that operator. I decided to test the system again. However, this time I would contact all of the providers. I decided to contact each major internet provider through two separate calls and document the results. My goal was to identify the personal information requirements for each provider in order to activate service to a residential home. The following were my findings. Please note that your experiences may differ.

I started with Comcast. I assumed that they would be the worst to deal with. This is probably due to years of negative publicity in reference to horrible customer support. They were actually quite pleasant. I stated on two calls with two different employees that I wanted internet service but would not provide an SSN. The first employee stated that an SSN was required for a "risk

assessment". I inquired on ways to bypass this requirement and discovered that Comcast will eliminate this requirement and risk assessment if the customer pays a $50 deposit. The deposit would be returned after one year of paid service. The second employee also stated that an SSN was required for a "risk assessment" and that there was no way to bypass this. I mentioned the $50 deposit, and after a brief hold was told that the deposit would eliminate the requirement. I have had two clients since these conversations who have confirmed that Comcast will provide service to any name supplied as long as a credit card deposit of $50 was provided. I consider this a fair compromise. Comcast also did not require a contract of any specific length of service.

I contacted many of the most common internet service providers in the United States. I asked a series of very specific questions in order to identify those that would allow an account to be created in an unconfirmed name. The table that follows this section displays my results. The categories of the table are explained below.

SSN Required: If the provider requires a Social Security Number (SSN), they will likely perform a credit check. This will associate your real name with the address of service.

DOB/DL Required: If the provider requires a date of birth or driver's license number, this is also a strong indication that a soft credit check will be conducted. This is likely a risk assessment at the least, and will also attach your name to your home. Using anything but your real full name will result in a denial of new service.

Contract Required: This indicates whether the provider requires you to sign a contract for service. This usually locks you in to a set period of time before you would be allowed to cancel. This is not a concern as far as a commitment to service. However, signing a false name here could get you into trouble in civil court. I discourage using any name aside from your own on any binding contract.

Deposit Required: This field identifies the deposit required in order to bypass the credit check mandated by most companies. Paying this amount, as well as the monthly service fee, ahead of service will often eliminate the requirement of a verification check of your name. I welcome a deposit requirement in lieu of providing personal details.

Credit Check Required: This column identifies the companies that absolutely require a full credit check. I have found no way to bypass this requirement with the providers listed. This will certainly associate your name to your address and will be present through online resources.

Prepaid Option: Only Xfinity Prepaid offered truly anonymous service without a demand for any personal information. This requires an upfront purchase of a modem and "refillable" monthly service. My only complaint is the 20 Mbps download and 1 Mbps upload speed.

Provider	SSN Required	DOB/DL Required	Contract Required	Deposit Required	Credit Check
AT&T	No	Yes	Yes	No	Yes
CenturyLink	No	No	Yes	$75	No
Charter	No	No	No	No	No
Comcast	No	No	No	$50	No
Cox	No	No	No	$40-$65	No
DishNet	Yes	Yes	Yes	N/A	Yes
Earthlink	No	No	No	Varies	No
Frontier	Yes	Yes	No	N/A	Yes
Verizon	No	Yes	No	No	Yes
XfinityPrepaid	No	No	No	No	No

Your experiences may vary from mine. Overall, most internet service providers stated that an SSN and credit check were required for service at first. When pushed on alternative options, many acknowledged that this information was not required. I found that the following two questions gained the best results when talking with a sales representative. I encourage you to be persistent. Overall, the person you talk to wants to complete the sale.

- I was recently the victim of identity theft and was told to no longer disclose my SSN. Is there any way I can provide a deposit instead of giving you my personal details?
- I reviewed your website offer details and I will be paying automatically by credit card in order to forego giving you my SSN or DOB. Is this still your policy?

SSN Alternatives

Whenever a utility service demands an SSN for a client, I often respond that the client is not a U.S. citizen (an actual scenario where this worked for a client is explained later). Sometimes, the utility will demand the equivalent number for that person's country. I am always prepared for this. Most utilities will accept practically any number you give them, but some will use an online service to verify the number conforms to the country's standard. Canada uses the Social Insurance Number (SIN) system. The following three SINs will verify as valid, but will never be assigned to anyone.

903 841 278 / 991 598 558 / 902 280 171

The United Kingdom uses the National Insurance (NI) number, and the following three NIs will verify as valid, but will never be assigned to anyone.

SX 87 58 64 B / KR 11 23 28 A / RY 61 81 33 D

Amazon

I place orders through Amazon weekly and never jeopardize my privacy during the process. If you are already using Amazon and have an account created, I recommend that you stop using that account and create a new one. The details which you provide are very important. Before discussing the appropriate methods, please consider an actual scenario.

A client had recently moved to a new rental house to escape a dangerous situation. She had nothing associated with her real name at the address. The utilities were still in the name of the landlord. She used a PO Box for her personal mail. She was doing everything right. She created a new Amazon account and provided the name of her landlord and her home address for shipping purposes. This way, her packages would arrive in the name of the property owner and she would stay invisible. She made sure that her name was not visible in any part of the order.

When prompted for payment, she used her real credit card in her name. She verified one last time that her name was not present anywhere within the actual order or shipping information. Her item, a pair of hiking shoes, arrived in the name of the landlord. Her real name was not referenced anywhere on the package. Within thirty days, she received a piece of mail that made her stomach drop. It was a catalog of hiking equipment addressed to her real name at her address. The company that accepted the order through Amazon was given her name as attached to the credit card. Therefore, the company added her to their catalog delivery list.

All of her hard work was ruined from this one mistake. Within another thirty days, she started receiving other junk mail in her name. Within ninety days, she found her name associated with her address online. This was her only slip. The lesson to learn here is that you can never tie your real name to your address if you do not want that association public.

The following steps will mask your real identity from your Amazon purchases. This technique can also apply to other online retailers. Create a new account with the following information.

- **Name**: Use the name that you want your packages shipped to. This could be the landlord at your address, or a new alias.
- **Email Address**: You must provide an email address for your new Amazon account. I recommend using the ProtonMail account created for home use as discussed earlier. This new Amazon account will never be associated with your real name, and it will not be connected with any of your real email accounts.
- **Payment**: My first preference is to purchase an Amazon gift card with cash from a local store. This is the least invasive option. If you must, a Privacy.com card could be used, which would provide adequate protection for most people.

- **Address**: Provide your shipping address as desired. This may be your actual home if you do not have a better place for deliveries. If you are ordering large items, it can be convenient to have them delivered directly to your house. My preference is to have all small packages delivered to an Amazon locker if you have one nearby. I have used my real home addresses in the past, but only for large deliveries. Because the name on the shipment is not my real name, I do not see this as a privacy concern. I believe it helps establish that someone else lives at your residence, and provides great disinformation. You should scrutinize any option you choose and make sure that it is appropriate for your scenario. Another option is to have packages delivered in your real name to your UPS box.

This method should protect you from any association between your name, your purchases, and your home. You could likely use this new Amazon account for all of your purchases and have no problems. However, I encourage you to take things a step further and apply a bit more paranoia to your plan. I create a new Amazon account after each gift card has been depleted. This way, Amazon does not have a single record of all transactions. Additionally, each Amazon account is in a new alias name for both shipping and billing. It will add disinformation to your address and will confuse your delivery person. The only drawback to this is if you subscribe to their Prime membership. You may want to create one account to be used solely with those benefits, such as streaming video. I prefer to avoid these services.

If you desire extreme privacy, I believe you should avoid any deliveries made directly to your home. When Amazon lockers are not available, consider shipping packages to your UPS store. This prevents any spillage of real payment information in association with the home. For an extra layer of privacy, I ship most packages to an LLC name similar to a real LLC that I listed on my registration form with UPS. This prevents me from associating my real name with the purchases, and the LLC is not connected to me through the state.

I realize this section offers many options without enforcement of a specific strategy. You should determine what is best for you. I will break down my preferred Amazon payment and shipping strategies in order from most private to least private.

Order: Alias Name > Payment: Gift Card > Shipment: Amazon Locker
Order: Alias Business Name > Payment: Gift Card > Shipment: UPS Store
Order: Alias Name > Payment: Gift Card > Shipment: Home
Order: Alias Name > Payment: Privacy.com > Shipment: Home
Order: Real Name > Payment: Credit Card > Shipment: Amazon Locker
Order: Real Name > Payment: Credit Card > Shipment: UPS Store

Moving Services

You will likely be asked to provide a credit card as a deposit when you reserve a company for any type of high value service. This may include home maintenance, satellite television, or movers. Many of these will not accept prepaid cards and will insist on a hold of funds within the credit card account. For these situations, I always recommend using your secondary credit card in an alias name. The following example illustrates the importance of not using a card in your true name with home services.

A client was relocating to another state to escape an abusive ex and to take on a new job. She was renting a small apartment near her new employer which included all utilities. She knew not to attach her name to anything regarding her new address. She contacted a popular home moving company and scheduled them to arrive at her current home, pack her belongings into a moving truck, and deliver them to her new address. As you can imagine, this presented a unique situation. They rightfully needed her current address and new address. They also insisted on obtaining her name, credit card number, and a telephone number to contact her during delivery. She panicked and hung up without giving them any details. Then she called me.

If she had completed the order, there would be a very strong trail from her previous address to her new address. I suspect that within weeks, she would receive targeted advertising in her name at her new address offering typical services to a new resident. Many moving companies supplement their revenue by sharing customer databases with non-competing services which cater to new residents. This data could easily leak to online people search websites. I decided to help her by facilitating the entire moving process on her behalf.

I chose U-Haul as the most appropriate mover for her situation. Her relocation was substantial, and the mileage fees alone for a moving truck were outrageous. When adding the fee for two movers to facilitate the transfer, the quote was several thousands of dollars. I completed the order for the move in three isolated phases. For the sake of this scenario, assume that she was moving from Miami to St. Louis.

I scheduled U-Haul to deliver two moving U-box containers to her current home. These are large wooden crates which allow you to store belongings before being shipped by a semi-truck and trailer. U-Haul required a valid credit card so I provided my client's secondary credit card in an alias name. This order also included pickup of the full containers and storage at the Miami U-Haul headquarters. The boxes were delivered by the local Miami U-Haul provider closest to her home.

She had friends help her fill the containers and I called U-Haul to come and pick them up. They were transferred and stored at the Miami headquarters awaiting further instruction.

Customers are allotted 30 days of included storage before additional fees are introduced. I called the Miami U-Haul and provided the order number and alias name. I requested that U-Haul deliver these containers to the St. Louis storage facility. I was given the rate for this service and a deposit was charged to the card on file.

A week later, the email address on file received a confirmation that the containers had arrived in St. Louis. They were stored there awaiting further orders. The storage fees were covered as part of the original contract. Through the U-Haul website, I identified a reputable moving company. I added their services to the current open contract and provided a destination address of a post office within the city near where she was moving. This was the last piece of information that was given to U-Haul. I authorized U-Haul to release the containers to the moving company.

I called the independent moving service that would be picking up her containers and delivering them to her new apartment. I provided the order number and her alias name. I stated that the original order had a placeholder address because I did not know the new address to where I was moving. I then gave this company her actual address over the phone and she met the movers there to direct them with the move. She possessed the release code that allowed the moving company to close the contract and be paid by U-Haul.

Out of curiosity, I input similar beginning and ending addresses within the U-Haul website moving calculator. My method was the exact same price as if I would have given U-Haul everything they needed in one step. In my method, U-Haul does not know her real name or her current address. For full disclosure, they know that she likely lives near St. Louis. There is very little value in this information to U-Haul. The independent moving company knows her new address, but they do not know her name or from where she moved. If her U-Haul account were to be breached, her address would appear to be a local post office.

I trained her to have small talk answers ready for the movers. She was to say that she is staying in St. Louis with her husband while he was assigned there by his employer and then returning to California soon. I later asked her how that went. She stated that she simply did not answer any of their questions and they stopped talking to her altogether. I liked working with her.

As you can see, every step of any relocation is full of potential vulnerabilities. One mistake can unravel all of your effort. Plan everything to the point of exhaustion. Attempt to find areas which may present hurdles. Run through every possible scenario and consider any ways in which your privacy may be in jeopardy. Again, this is a lot of work. However, the payoff at the end is worth all of the hassle.

Appliance Purchases

During a move, it is likely that you will need some major purchases delivered to your home. There is no room for error here, as most big-box stores collect and share data about all of their customers. When you purchase a refrigerator, washer, dryer, or other large item, free local shipping is often included. In order to complete the delivery, the store will require your home address, telephone number, and a name. The address must be accurate, but you could provide a burner phone number and an alias name. However, the name provided must match the source of payment. If you use a real name or accurate credit card, you have just connected your true identity to your home address.

In previous books, I have mentioned the ability to make the purchase under an alias name with a secondary credit card, but I no longer have faith in the protection this provides. In 2017, I needed to purchase a replacement oven for a non-functioning unit. I had agreed to complete this task for my landlord as part of his willingness to allow me to stay there anonymously. I walked into a national chain appliance store and identified the model I desired. I had no way to transport it to my current rental unit. During checkout, I provided my alias name, which also appears on my secondary credit card. When the sales person swiped the card, he asked if any of the names on the screen were me. The first option was Michael Bazzell. Since I am always concerned about protecting my home address, I awkwardly canceled the order and left without completing the purchase. Fortunately, I had not yet provided the delivery address. This was a close call.

What happened was a careless mistake. On a previous visit to this chain at another location, I used my real credit card under my real name to make a small purchase. This entered me into the nationwide system. Since my alias secondary credit card possessed the same account number and expiration as my primary card in my name, the store knew both purchases were connected to the same card. The system queried the card number and prompted the sales associate to choose any applicable names of previous customers. Some stores do this with telephone numbers. While this may seem minor to your threat model, it was a serious violation to me. Today, I conduct these purchases quite differently.

I first visit the store to identify the exact appliances I desire. I make sure that my choices are in stock and ready for delivery. I choose businesses with powerful online stores such as Lowe's and Home Depot. I then leave and decide which level of privacy I desire for me or my client. I present two options here, displayed in order of most private to least.

If possible, I make the payment in store with cash. I then provide the real address for delivery and any name I choose. Some stores will not accept cash over a specific limit and will decline a large purchase. While the money displays "legal tender", private businesses have a right to refuse cash. My next option is prepaid credit cards. I purchase enough gift cards to cover the

entire amount, and again provide the real address with an alias name. This has worked throughout most of 2017 and 2018. Lately, I encounter stores that require government identification in order to schedule a delivery. This is a deal-breaker for me. When I receive this level of verification, I move to the second option.

I make the purchase through the store's website using a Privacy.com debit card number. We lose a small amount of privacy here because there is a digital trail back to my bank. This is acceptable for most clients. After the online purchase is approved, I telephone the local store and schedule the delivery. Since I am not there in person, there is no way to enforce a check of identification. The delivery people could ask for it, but this has never happened. If it did, I would simply claim that I didn't have one with me, as I was not told this would be a requirement.

Using Privacy.com debit cards online is not always possible. Beginning in late 2018, I noticed more online stores were declining debit card numbers generated by Privacy.com. This is because these numbers are clearly tagged as an anonymous payment type, similar to a prepaid card. When a merchant processes a payment with one of these cards, it may have rules that decline the purchase completely or if above a specific amount threshold. This has happened to me, but there is always a workaround.

I attempted to purchase a refrigerator from Home Depot through their online website. I knew it was in stock locally and I planned to have it delivered at no cost. I provided my real address, the name of John Wilson, and a VOIP telephone number assigned to my home. The purchase was immediately declined. I knew that the Privacy.com card I was using was valid and had not been used with any other merchants. The Privacy.com app did not display any declined charges. A call to Home Depot customer support only revealed that the purchase was declined, with no further explanation.

I called the local store, and asked to speak to someone in the home appliance division. I explained that I tried to make a purchase online, but that it was declined. I told the employee that I contacted the bank that issued the debit card and was told there was no attempt to process the charge from Home Depot. I then asked if they could do this manually. The employee agreed and processed my order over the telephone. I provided the same Privacy.com card number, alias name, and actual home address. The charge was processed with no issues, and I could see the transaction within the application. The refrigerator was delivered two days later without incident, and I was never asked to display identification. The receipt was scanned into a PDF at the store and sent to my ProtonMail email address assigned to my home.

I should note here that a Privacy.com account has an initial purchase limit of $300 per week. This will not suffice for large purchases. Once you routinely make small successful purchases using this service, your limit will slowly rise. I have found that a call to their support can lift

that limit higher. I have clients who are allowed to spend up to $2,500 weekly with a monthly limit of $10,000. It takes time to build to this level, so I suggest using the service long before it is needed.

Overall, I never associate my true name with any delivery to my home address. This includes products paid for using a secondary credit card which could easily be tied back to me. In the first scenario (cash or prepaid cards), my weakest link is the surveillance footage of me in the store. If they demand government identification, this option cannot be made private and should be avoided. In the second scenario, the Privacy.com card is my threat. Privacy.com knows my name and that I purchased an item at a specific store, but does not know my address. The store knows I purchased with a Privacy.com card and my address, but does not know my name. The bank knows I spent money through Privacy.com. A court order to all three would reveal the connections. For most clients, that is not a violation of their threat model. For a rare handful, it is. Consider the following situation I had with a client.

In 2018, I helped a client who was an ex-wife of an FBI agent who had begun harassing her online and in real life. She worried that his access to premium data mining tools and government databases placed her at an increased risk. When she purchased her appliances with delivery to her new anonymous home, she ordered one item at a time, always paid cash, and politely declined to display any identification during each purchase. She is a focused, strong woman who can tolerate awkward moments and silence. Her cold stare magically bypassed the ID requirement each time. She is a ninja, so your mileage may vary.

Some clients express concern over the warranties which come with appliances. Large items often include a warranty card which must be mailed to the manufacturer. It asks for your name, address, and telephone number, along with a serial number of the appliance. My clients ask if they should use their real names since a warranty in an alias may create a situation where payment cannot be processed. My firm stance is that these cards should be avoided. They are not required for the warranty to be active, and seldom change any of the coverage. Your receipt from the purchase will satisfy any requirements, and the date on the delivery receipt defines when the warranty begins.

When I had a clothes dryer stop working within the warranty period, I simply called the local store where it was purchased and requested a warranty repair or return. The store was able to view my purchase history under the alias name and accurate address. The store created a service ticket, and a third-party repair company contacted me. They responded to my home the next day and repaired the machine. They already possessed my alias information because Home Depot shared it with them. This did not surprise or concern me, as it was an alias name. This is another example of how any details provided at the time of purchase can be shared without your knowledge. Your diligence with anonymous purchases will protect your home address from being publicly exposed.

Medical Services

This section presents quite a quandary. Until this point, I have encouraged you to hide your true identity during purchases in order to protect your personal information from being released publicly. Medical services can complicate this rather quickly. Your doctors need to know your true identity in order to update health records which could be vital to your life. Health insurance requires confirmation of your identity including photo identification and an SSN. We are often told by medical staff that HIPAA laws protect our information, but the countless healthcare breaches prove this line of thinking as incorrect. We know that any information provided during receipt of medical services is likely to be stored insecurely, shared intentionally, or leaked accidentally. Therefore, let's clean it up.

If you need emergency services, surgery, or typical care from a physician, I believe you should absolutely provide your true name and DOB. This will be used to modify patient records, and during any follow-up care. For me, the personal details stop there. I never provide my SSN, home address, personal email address, or telephone number in any circumstance. The following actual events should summarize my reasons.

In 2017, I visited a local optometrist for an eye checkup. I provided my real name and a slightly altered DOB. I refused all other details and paid with cash. The office insisted I provide a cell number as it was the system identifier. I supplied an old Google Voice number which was no longer used. Within 90 days, I began receiving marketing text messages related to eye care. Today, my true name is associated with that phone number within a marketing database titled "U.S. Consumers" provided by infousa.com. I can do nothing to remove it. Fortunately, the DOB and contact information does not jeopardize my privacy.

In 2018, I responded to a local urgent care facility due to suspected pneumonia after extensive international travel. I provided my true name and DOB on the patient paperwork. I supplied a VOIP telephone number, a CMRA mailing address, and a burner email address. I left the SSN line blank. When pushed for my SSN, I explained that I was paying cash and that I had not met my (high) deductible on my health insurance. I was treated, medicated, and released. In less than 90 days, I received an email to my burner account from "DrChrono" urging me to get a flu shot at the same urgent care facility where I was previously treated. It referenced a high number of flu-related cases which can lead to pneumonia. DrChrono is the software solution used by many urgent care facilities to collect and update patient information. I never agreed to provide my name, email, or location to this third party, yet it was shared. I still receive targeted advertising from that visit. Should I really care about this company knowing my medical history? I believe so. If you disagree, consider the following verbatim wording from their privacy policy:

"We use information, including Personal Information, for internal and service-related purposes and may provide it to third parties ... We may use and retain any data we collect to provide and improve our services … We may share any information we receive with vendors and service providers … If we are involved in a merger, acquisition, … your information may be sold or transferred."

In other words, they can do anything they like with your medical data. Worse, the collection of data is more likely to be breached or leaked publicly. The next week, I responded to a local pulmonologist for follow-up to my issue. As expected, they demanded many personal details. I provided a unique email address and VOIP number as well as the same CMRA mailing address. I attempted to leave the SSN line blank, but I was challenged. I was informed that this was mandated by federal law (which is not accurate) and required from insurance providers (which is also not true). My line about my deductible was not getting me anywhere. The compromise I made was to supply my health insurance account number, which could be verified on my member card. The office staff hesitantly accepted this.

In 2019, I was sent a notice from this office notifying me that the physician I had seen was retiring. I didn't think much of this as he was not someone I planned to visit again. Three weeks later, I received promotional emails and text messages from other area doctors who could take over for any related medical needs I had. I assume that the original office sold their patient contact data to similar offices before shutting the doors permanently. This was likely a HIPAA violation.

If you are often forced to provide an SSN for medical treatment while paying with cash, you have an alternative option, which enters some grey area. You could apply for an EIN from the IRS. I have a client who has done this. He grew tired of the battle to exclude his SSN from new paperwork with every visit. He applied for a Sole Proprietor EIN from the IRS, which was approved instantly and included a confirmation letter from the IRS displaying this number. He now provides this EIN, which is the same number of digits as an SSN, on all of his forms. He also provides his insurance card which displays the unique number assigned to him for any claims. The medical offices have no idea that the number he provides on the SSN line is actually an EIN. Both pass validation. Since he owns that number, he is not committing fraud. However, there could be some issues with this. If his insurance provider receives notification that treatment was conducted for a person with the EIN he supplied, the claims could be denied. Some medical services only include the insurance ID number within claims while other place priority on the SSN. If he were challenged by his insurance provider, he could provide proof of the ownership of the supplied EIN, and could say that he accidentally gave that instead of the SSN. I only tolerate this strategy for those with minor medical needs. Do not risk continuous treatment over SSN formalities such as this. Remember, EINs can be identical to SSNs of other people. Tread carefully. Finally, your health is more important than all privacy measures.

Anonymous Purchase Complications

I have experienced many failures while attempting anonymous purchases. Beginning in 2018, I started seeing a huge increase in blocked payments, especially if ordering physical products via the internet. When using a VPN connection, burner email address, alias name, and VOIP telephone number during an online order, I found many purchase attempts blocked by various fraud prevention strategies from the merchant. My orders were canceled without explanation. This happened even when using a legitimate payment source. Since then, I have documented the most common traits of anonymous payments which seem to trigger fraud prevention systems.

- **VPN**: A VPN alone will usually not flag a payment as fraudulent. In my experience, there must be additional factors before this makes an order seem suspicious.
- **Name**: If using a legitimate credit card, the name must match perfectly. If using a secondary credit card, the alias name must also be exact. Your credit card company discloses to the merchant if the name is different than on the account.
- **Email**: If using a known temporary email provider (such as Mailinator) or masked service (such as 33Mail), this will cause scrutiny. In my experience, legitimate alias email options from ProtonMail and Fastmail will be accepted. Credit card providers do not always confirm registered email accounts with the merchant.
- **Address**: Providing a shipping address different than the billing address causes scrutiny. If the shipping address is a CMRA or PO Box, expect even more hesitation. Combine a UPS box with a billing address in another state, and you should expect a blocked payment and canceled order.
- **Telephone**: When you make a purchase with your credit card, you are asked for a telephone number. The merchant will be notified if that number does not match the number associated with the credit card account. Therefore, I attach secure Google Voice numbers to my credit cards associated with my real name and secondary alias names. I then provide the appropriate number on all orders.
- **Prepaid Cards**: I only use these for purchases inside physical stores. Online use requires registration and often an SSN. Online orders with a prepaid card will be blocked without proper registration.
- **Masked Cards**: Companies know when you pay with a masked card such as Privacy.com. Many online merchants will block purchases unless the billing name matches the shipping name, and the shipping address matches public people search records.

The following examples summarize actual successes and failures when ordering products through online merchants.

- I attempted to purchase several refurbished iPhones directly from Apple. I provided a legitimate Privacy.com card number, alias name, and UPS store address. The order was canceled due to "high risk". Talking with the Apple security team revealed that the suspicion was because the name provided did not specifically match the payment source or address. While Privacy.com allows you to use any name for purchases, merchants can block these payments due to lack of a confirmed name through public records and online databases.
- I attempted the same type of purchase through Gazelle. The order was canceled immediately. Fraud prevention personnel confirmed that the cancellation trigger was because the payment source was a masked debit card. They confirmed they would not accept any prepaid or masked card which were not registered to a real name, address, and SSN.
- I attempted to order several discounted new iPhones through Best Buy. I provided my secondary credit card in an alias name, a shipping address of a UPS store, a VOIP number, and an alias ProtonMail email address. The order was canceled because the telephone number did not match the number associated with the secondary credit card, and the delivery address was in a state different than the billing address.
- I attempted another purchase directly through Apple. I used my secondary credit card, exact alias name displayed on the card, exact billing address (PMB), a UPS store shipping address, and the VOIP number on file with the alias credit card. The order was accepted, but held for review due to the shipping location being a UPS store in a different state than the billing address (PMB). Apple demanded a call to me at the number on file with the credit card. I answered the call (forwarded to MySudo) and confirmed all aspects of the order. The phones shipped the next day.

The lessons learned are as follows:

- Many online merchants will not ship products when using masked or prepaid payment options. Calling a local store will usually bypass this restriction.
- Merchants will accept traditional secondary (alias) credit cards if all provided information matches records provided by your credit card company.
- Be prepared to accept a call at the number provided during purchase, and make sure that number is on file with your credit card provider.
- When an order is canceled, call support and challenge this annoyance. Often, orders are canceled due to suspicion of fraud, and the merchant assumes that a criminal will not challenge the decision. Contacting a human over the telephone often eases the level of concern for fraud. You can request that the card used be "whitelisted" for another order attempt. If approved, you can then repeat the purchase and hope for a better result.

Post-Purchase Considerations

Over the past few years, I have witnessed a concerning interaction between the merchant and customer after a purchase has been made. This is usually in the form of an unsolicited text message or email from the merchant asking for feedback about the purchase. These are extremely common in the service industry, including everything from home repairs to medical appointments. Consider the following two scenarios which jeopardized the privacy of my clients in 2019.

"Joan" purchased a WordPress plugin for her online business. This premium option allowed her online blog to easily accept credit card payment for a niche product she provided for sale. During checkout, she supplied her real name, credit card details, burner email account, and the PO Box address near her private home. Joan was not under any threat of physical violence, but desired a basic level of privacy. There was no public online documentation of the city and state where she resides (yet). Within minutes after the order, email messages began arriving about her purchase.

The first was a welcome message explaining use of the product and the required license key. Immediately following, she received an automated email from a sales representative requesting feedback about the purchase. She ignored this message. The next day, she received an email message asking if there was something wrong with the purchase. The wording insinuated that a confirmation was required in order to use this product, and specified that they had not heard from her since the purchase. She responded "Everything is working fine for me, No issues".

She immediately visited the website to make sure she could still log in to the portal, and noticed something inappropriate. On the home page of the site, a section titled "Happy Customers" displayed a scrolling list of people who had recently purchased this plugin along with a brief snippet of feedback. For Joan, it displayed her first and last name, city and state, along with "Everything is working fine for me, No issues". She was appalled and immediately contacted the company demanding removal of the content. The response from the company was that this was standard marketing, and that she agreed to the use of her information. The employee provided a link to their privacy policy page, which indeed included wording about use of customer feedback on the site. Joan's approximate location was now publicly visible to the world. It was eventually overridden with more recent feedback.

"Mark" visited a new dentist for a routine exam. He was new to the area after he relocated to an anonymous home upon receiving numerous death threats and a violent physical attack. He chose a dentist in the town adjacent to his home, and used his real name to make the appointment. He provided a PO Box as an address, VOIP number for his cell, unique ProtonMail account for his email, and paid with cash. It is important to note that Mark's real

first name is very unique, and there are only a handful of people in the country with that first name. This will work against him in a moment.

Days after the exam, Mark began receiving text messages from the dentist's office in reference to his visit. They were requesting feedback from him in an effort to provide the best experience possible for all patients. He ignored these, but they kept coming. They started with, "We would like your feedback", became more aggressive with, "We still need you to respond", and finally became invasive with, "Your input is required". Mark finally responded to the messages in order to make them stop. He submitted something very generic such as "Great visit". The messages finally stopped.

Several days later, Mark conducted his weekly search of his name on Google. He does this to identify any new threats toward his privacy. He used the "Past Week" option in the "Tools" section of Google in order to filter results to only those posted in the past week. The first result made his stomach drop. It was a review site for the dentist Mark had visited. One of the recent reviews was, "Great visit", and it was attributed to Mark's real first name and last initial. The page clearly identified the city and state where the office was located, and Mark was now exposed.

Some may think this is no big deal, but I feel different. The service requesting feedback from Mark never asked for consent to publish the information. This may have been included in the paperwork signed at the office, but Mark could not recall any wording associated with this action. Publishing the first name and last initial would be less invasive to a person like me (Michael B.), but Mark's real name is immediately distinguishable at over 15 characters. Anyone searching his name now has a great starting point to find his home, as very few people visit a dentist while on vacation.

Fortunately for Mark, I was able to have the feedback removed. I first contacted the dentist's office and made a polite request on his behalf. The office staff informed me that they do not have control over that data, and that they hire a third-party company to send those messages, collect the content, and publish to a dental review site. I contacted the business providing this service and repeated my request. I heard nothing back from them, and had my attorney draft a cease and desist letter to them demanding removal of the information or accept the risk of civil litigation. The content was removed the next day, but I never received an official response from the company. A letter from an attorney is most often a bluff, but usually not worth fighting.

You have probably received similar messages from a merchant after a payment. With the popularity of review websites such as Yelp, TripAdvisor, and many others, businesses want to stay ahead of any negative reviews. By convincing happy customers to submit positive

feedback, they often have a legal right to publish the content you provide. These positive reviews help drown out the negative feedback initiated by unhappy customers.

I believe there is never a reason for a privacy-conscious person to provide any type of review or feedback in any form. Whether directly to the merchant or on a third-party website, you are exposing potentially sensitive information when you volunteer any details about your purchase or experience. Furthermore, you have nothing to gain. The only party which benefits from your feedback is the merchant. In most scenarios, merchants are hiring third-party companies to send these messages and collect the data. You have no control over the ways this data is abused. A breach, leak, or intentional sale of the data could expose you to numerous online people search websites. The simple solution is to never participate in this activity.

Virtual Currencies

You may question my reasons for excluding virtual currencies, also known as cryptocurrencies, such as Bitcoin, from the beginning of this chapter as a private payment option. First, I have found most services to be too complicated for most of my clients. Second, possessing truly anonymous digital currency can be quite complicated. Let's begin by defining virtual currency. It is a type of unregulated digital currency which is issued and usually controlled by its developers. It is used and accepted among members of specific virtual communities. The most popular, and most widely accepted, is Bitcoin. Next, we should acknowledge the typical route most people take to purchase this digital money.

Most people who own any type of virtual currency purchased it through an exchange. You might create a profile, provide a credit card number, and purchase a specific amount of Bitcoin. The currency is placed into your "wallet" which is maintained at the exchange. You can now spend this money anywhere which accepts Bitcoin. The merchant does not know your identity, and the Bitcoin is "anonymous". However, there are many concerns with this strategy. First, the exchange will demand to know your true identity. You will be forced to upload government ID and third-party verification systems will confirm any inaccuracies. Next, the exchange will maintain a record of all purchases. A subpoena to them would disclose all of the activity associated with your name. After that, the publicly visible wallet identifiers disclose the exchange service you use. Finally, you are at the mercy of the security practices of the exchange. Numerous companies have suffered data breaches which lost all of their customer's money. All of this takes away any privacy benefits of virtual currency. I believe all exchanges should be avoided if you want true anonymity.

I prefer to control my own locally-stored Bitcoin wallet. This can be done with **Electrum** (electrum.org), an open-source software application which stores, accepts, and transmits virtual currencies directly from your computer. Let's walk through installation and transmission of Bitcoin through Electrum. You can download the software from their official

website. It natively supports Windows, Mac, Linux, and Android, and the installation is straightforward. Next, we need to create a wallet.

- In the Install Wizard, click the "Choose" button to identify the default directory.
- Click "Cancel" and enter the desired name of your wallet and click "Next".
- Choose a "Standard Wallet" and click "Next".
- Select "Create a new seed" and click "Next".
- Accept the default seed type and click "Next".
- Copy the words presented into a password manager for safe keeping and click "Next".
- Paste the words into the next screen to confirm receipt and click "Next".
- Choose a secure password, enter it, and store it in your password manager.
- Click "Next" and close the application window.
- If desired, move your wallet file to a more secure location.
- Open the application and ensure you can access your new wallet.

Congratulations, you now have a Bitcoin wallet. However, you have no Bitcoin. This is the hardest part. If you cannot buy virtual currencies from an exchange, how do you get any? Some people use Bitcoin ATM machines. You can insert cash and provide a Bitcoin address for deposit into your account. The disadvantages are a 5% to 10% fee for this service and the potential of making a mistake and losing any money. Furthermore, many people report machines requiring you to take a "selfie" while holding your ID, which I would never recommend. However, if you have a local ATM and want to experiment, here are the instructions.

- In the Electrum application, click the "Receive" button at the top of your wallet.
- Copy the receiving address, similar to "1IKIV7Anhsv15RXYS7X2HR2ijjMV7BzIsI".
- Enter a description of the transaction, such as "ATM" and click "Save".
- Click the barcode to enlarge and print the visible barcode.
- At a Bitcoin ATM, follow the prompts to scan your barcode or enter your Bitcoin address, enter the amount of purchase, insert your cash, and confirm your deposit.
- In a few moments, you should see a pending deposit within the Electrum app.

There are a couple of things to explain further. Electrum needs internet connectivity to connect to the Blockchain in order to update any transaction records. Many ATM machines demand a cellular telephone number in order to send a text message containing a code which needs to be entered into the ATM. You could use a VOIP number as explained earlier, but this now associates the transaction with that number. For this reason, I try to avoid ATM machines unless I need the funds available right away. The confirmed Bitcoin deposit can take hours to become available within your wallet.

My preferred way to acquire Bitcoin is from another individual. This can be accomplished in a couple of different ways. The best option is to provide a service which can be paid via Bitcoin. For several years, I provided an online training program which accepted Bitcoin. This helped generate my first few Bitcoin transactions and allowed me to build up my wallet of funds. If you have an online service that caters to privacy enthusiasts, accepting Bitcoin can benefit both you and the consumer.

Technology, hacker, and even Bitcoin-themed conferences are common in urban areas. These events usually include a Bitcoin party where virtual currency enthusiasts gather. One purpose of this interaction is to buy and sell Bitcoin. Many people will happily sell their Bitcoin for cash while buyers see this as a great opportunity to obtain fairly anonymous money. Be careful. Make sure there is a trusted mediator present to ensure the transaction goes through. It is important to have access to your wallet in order to verify the transaction. Ask other attendees about trusted sources and identify someone with whom you feel safe making an exchange. After attending a few events, you will get a feel for the reputable providers. The process within Electrum is identical, and you would give the seller the address or barcode.

Let's assume you now possess some Bitcoin. What should you do with it? For most of my clients, not much. Less than 5% of my clients possess any virtual currency. Of those, very few ever spend it. The most common uses for cryptocurrency are online services and exchanges. You can buy a VPN service, ProtonMail account, or online storage solution with Bitcoin without disclosing a true name or credit card. However, very few physical retail locations accept it. I keep Bitcoin available at all times in order to anonymously purchase these types of online services for clients. Paying via Bitcoin removes most identity verification demands. In order to spend Bitcoin stored in Electrum, the following should assist.

- Click the "Send" option at the top.
- Enter the Bitcoin address provided by the service you are purchasing.
- Provide a description and amount.
- Click the "Send" button.

Be careful with the amount. You can use various online conversion utilities to display the amount of Bitcoin in USD, or you can add USD as an option directly within Electrum. The following modification in the software adds USD in the send, receive, and balance menus.

Tools > Electrum Preferences > Fiat > Fiat Currency > USD

Any virtual currency you possess in this wallet is your responsibility. If you delete the file or lose access, you have lost any money inside it. It is estimated that 23% of all Bitcoin has been lost due to inaccessible wallets. Please do not become part of this statistic. Overall, most of my clients have no use for Bitcoin. I only recommend these actions if you truly NEED it.

Summary

Is all this effort really worth it? For me, absolutely. I value the privacy benefits of a truly anonymous home. For my clients under threat of physical danger, of course. Their lives may depend on absolute invisibility. For you…well only you can answer that. I will leave you with one final scenario to end this chapter. The following happened to a close friend and colleague two days before I wrote this section.

"Mary" returned from vacation to discover a concerning series of emails. An internet stranger, whom I will refer to as "Jack" had been attempting to reach her through her LinkedIn profile. Jack was selling a guitar on the mobile app LetGo and had been contacted by a potential buyer. The buyer sent a check to Jack for the purchase amount from a legitimate company with no ties to Mary. However, the "from" address on the FedEx shipment of the check included Mary's full name and home address. It was made to appear that Mary was the person purchasing the guitar, and Jack now knew her full home details.

Jack assumed this was a scam, and suspected Mary may also be a victim. Mary assured Jack she knew nothing of this purchase, and Jack contacted the company identified on the check in order to confirm it was counterfeit. Mary may not technically be a victim, as she lost nothing, but her identity was used during the execution of a felony. The abuse of her name and home address as part of a scam bothered her. While not living completely anonymous, her operational security was strong, and she was much more private than the average person. She wanted to know why she was selected, and how the suspect found her home details.

When Mary contacted me to look into this, I did not suspect a traditional people search website. She is not listed in those, especially under her home address. Since I possess numerous data breaches as part of my online investigations service, I went straight for those. A search of her name, which is quite unique, led me to the HauteLook breach discovered in 2019. HauteLook had 28 million unique accounts breached in August of 2018, including full names, home addresses, genders, dates of birth, and password hashes. This data was sold in underground criminal communities. I confirmed that her full name and home address in the HauteLook breach matched the information provided about her on the FedEx label.

Mary had never heard of HauteLook, but confirmed the email address on file in the breach was her personal Yahoo account. I asked if she ever shopped at Nordstrom, which she confirmed. Nordstrom owns HauteLook, and HauteLook fulfills online orders placed through Nordstrom's website. This was likely the connection. In other words, all of the details she provided for an order through Nordstrom were available to criminals, and likely being abused to make scam attempts seem more credible. There is nothing Mary can do to remove herself from this breached data. She can only change her habits from this point forward.

Her experience worsened a few days later. Mary received a $4,000 invoice from FedEx demanding she pay the shipping fees for the numerous fraudulent shipments made in her name. The offender(s) created an account in Mary's name at FedEx, and opened a line of credit by providing her full name, address, and date of birth (all available in the HauteLook breach). This account was used to send multiple checks via overnight shipping without expense to the criminals. This was now full identity theft.

If she had used an alias name during her online orders, she would be less exposed. If she had the shipment sent to a CMRA or PO Box, her home address would not be abused. If she had done both, an internet stranger would not have been able to contact her. While his intentions were good, I see many internet victims which wrongly believe people such as Mary are part of the scam. I have investigated crimes where one victim attacked another, suspecting foul play. If we cannot be found, we have very little to worry about.

If she had established a credit freeze on herself, FedEx may have declined the line of credit in her name. A credit freeze is vital for all Americans, and I explain the entire process in a later chapter. I want to make it clear that I do not place fault on Mary. We have all made privacy mistakes, including myself. I recall the days where I ordered packages to my home in my real name. None of us have always executed the most private strategies. We all start somewhere. Will this encourage you to start being more private today?

International Considerations: Every day, someone contacts me about anonymous payment strategies outside of America. As a U.S. citizen, working in the U.S., and helping mostly American clients, I simply do not have much experience with masked payment services in other countries. If your country does not offer secondary credit cards or virtual options such as Privacy.com, I believe your best option is to possess a business credit card. Most international banks will issue cards in a business name for numerous "employees", and will only require the detailed information of the business owner (you). The bank will know every detail of each transaction, but the merchants which accept the card are shown only a business and employee name (alias). Please use the details presented here to create your own solutions. Some readers have reported that **Revolut** (revolut.com) offers virtual cards in alias names throughout Europe. However, this requires a premium account with a $10 monthly fee.

I hope this chapter helps you dive into the world of anonymous payments. Once mastered, these strategies will prevent information leakage, and will keep you off of various public people search websites. Remember, it only takes one mistake to unravel all of your efforts toward anonymity. Merchants have a financial motivation to share your information with other merchants and service providers. Marketing and advertising are more difficult thanks to our tendencies to skip commercials, block online ads, and refuse to answer telemarketing calls. Companies now rely on your data in order to make a buck. You can combat this with anonymous purchases, and by never associating your real name with your home address.

Chapter Ten

Private Home Network

You are likely no stranger to the importance of virtual private network (VPN) applications on your computers and mobile devices in order to protect the identification of your true IP address. This numeric value associates you and your internet browsing behaviors to a unique identifier. It can be used to document your location and track you through every website you visit. Hopefully, you have already included a VPN as part of your privacy strategy. This secures your internet connection and anonymizes your activity online from any device which you have properly configured the VPN application. What happens if the VPN app crashes? What about network connections which cannot take advantage of a standard VPN application?

Think for a moment about the additional devices that are networked within your home. The wireless router that contains proprietary software, manufactured by a huge corporation, has unlimited access to your internet connection and can "call home" whenever desired. How about that mobile tablet which your children use to play free games? Those also likely collect your internet connection information and store it indefinitely. Do you have any appliances, such as a television, thermostat, or lighting system, which connect to your Wi-Fi in order to stream video, remotely control the temperature, or dim house lights from your phone? Not only do all of these connections announce your true IP address to the companies that made them, but traditional VPNs cannot be installed on the devices. Furthermore, we rarely update the software on this specialty hardware, and many devices possess security vulnerabilities waiting to be compromised.

Every time we add an internet-enabled device to our homes, we present another attack surface to our security and privacy. This is why I believe that every home should possess a digital firewall between the primary internet connection and every other device. I can use this for two specific protection techniques. First, this firewall will prevent any outside intruder from "seeing" or connecting to the devices in my home. This will likely prohibit the remote features of these products, which I believe is a good thing. Second, and most importantly, I can create a virtual private network connection for the entire house. Every device will be protected, regardless of its ability to possess and utilize VPN software.

I strongly advise reading this entire chapter completely before taking any action within your own home network. Throughout this chapter, I will be demonstrating both ProtonVPN and Private Internet Access (PIA) as my chosen VPNs for the configurations. I have found these

to be the most stable VPNs for router-based installs with automatic reconnections and great speed. This will be explained in more detail later. While I prefer ProtonVPN in regard to extreme privacy and security, their service is more expensive than PIA and some people report a higher rate of disconnections within a firewall. I have not witnessed this in the past year. I encourage you to test any current VPN you use within this tutorial. You only need ONE VPN provider for this technique, and I believe either ProtonVPN or PIA gets the job done.

The goal of this chapter is to create an instance of a single pfSense firewall, which will be the only device in your home that connects to the internet directly through your internet service provider (ISP). If you have a cable modem, it will connect to this new firewall. Every other device in your home will connect to the firewall, and be protected with an IP address provided by your VPN provider. No device in your home will ever know the IP address from your ISP. Please note that this chapter has appeared in my other books on privacy and security. However, there are many modifications to this tutorial, and they should replace any previous writings. I firmly insist that every client of mine who is living anonymously possesses this setup. Below are a few examples of how this technique can protect your anonymity.

- Mobile devices: If you connect your iPhone to your home Wi-Fi, Apple receives and stores the IP address attached to your home. Without a firewall containing a VPN, Apple knows your true IP, the area where you reside, and your ISP. This quickly associates your Apple account with your home address. A home firewall prevents Apple from ever knowing your true details.
- Laptops: Whether you use Apple or Microsoft products, they both send numerous details about your connection to their data collection centers, including your IP addresses. Again, a home firewall prevents them from ever knowing your true details.
- Media Centers: If you connect to Netflix, Hulu, or Apple TV through your home internet Wi-Fi, you are constantly sending out your true IP address of your home. Since you pay for these services, your payment method, home IP address, and billing details are merged and stored forever. By connecting these streaming services through a firewall with a VPN, you stop providing your home's unique IP address to the providers. Instead, you provide a VPN address which is shared with thousands of people all over the world. Some of these providers block VPN addresses, but I will tackle this later in the chapter.
- Appliances: We hear about how most new refrigerators, smart televisions, and video-monitoring doorbells connect to the internet to "assist" your daily life. A home firewall prevents accidental true IP address exposure.

Before discussing the software, I should mention hardware. In order to take full advantage of the bandwidth available through your VPN within a router, your hardware device needs to have a powerful processor, ample RAM, and a solid-state drive (SSD). This firewall is basically an entire computer. You could repurpose a desktop into a pfSense build, but this will consume

a lot of power for a single task. You could also rely on a virtual machine, but this requires a stable host. Instead, I highly recommend a custom **Protectli Vault**, which was created for this purpose. The unit which I provide to most clients is the 6-port FW6B (http://protectli.com). The 2-port and 4-port versions would also work great, but I place focus on the most applicable model available. Personally, I rely on the 6-port model for my daily use and occasional advanced needs. Whatever you choose, always ensure that your device has a CPU that supports AES-NI. Also, consider your internet speed. If you have gigabit internet and a VPN which supports such high speeds, you will want a 6-port Vault, as it offers faster VPN performance. The 2-port and 4-port models can only handle VPN speeds up to 250mbps.

I interviewed Brent Cowing, the CEO of Protectli, on the podcast in 2017 and learned about his company when I was looking for the most appropriate solution to my home router needs. These devices are very compact and act as their own cooling device. There are no fans or any moving parts; they are silent; and they require much less power than desktops. The model that I chose for testing contained 8GB of RAM and a 32GB MSATA solid state drive. I have had a Protectli box running almost non-stop for three years.

The following instructions walk you through the entire installation and configuration of a pfSense firewall with a VPN in kill switch mode on this specific device. This means that if the VPN fails, the internet stops working on any of your devices. This ensures that you never expose your true IP address. These instructions were replicated on the currently available latest stable version of pfSense, 2.4.5. Later versions may display minor differences, but the principles of this setup should apply to future releases. For those readers who have already read my writings on this topic in previous books, you will see some identical information. However, there are substantial changes in this version which should be considered.

Regardless of whether you have adopted the privacy and security strategies throughout this book, I recommend that you seriously consider the tutorials in this chapter. We all use the internet, and we all have numerous devices. The absolute easiest way to track your online behaviors is through your home IP address. A cheap VPN application is not sufficient. We need stable protection and a backup plan if a VPN connection should fail. This chapter solves these issues.

The content here is presented in several phases. I recommend practicing on your device as you go through these, without connecting it to the internet. When you feel confident you understand the techniques, reinstall the software and start over. This will ensure that you have made deliberate changes which you understand, and provide a deeper understanding about the software. **Many readers skip this chapter until they are ready to dive into the technical world of configuring a home firewall.** At the end of this section, I present a page on my website which allows you to download custom configuration scripts which simplify the entire process.

Phase One: Installation: Install the firewall software

The following steps download and configure pfSense onto a USB device.

- Navigate to https://www.pfsense.org/download.
- Choose "File Type: Install", "Architecture: AMD64", "Installer: USB Memstick Installer", "Console: VGA", and "Mirror: New York".
- Download the ".gz" file and decompress it (typically by double-clicking it).
- If your OS cannot decompress the file, download and install 7-zip from 7-zip.org.
- Ensure you have a file with an .img extension, such as pfSense-CE-2.4.5-amd64.img.
- Download and install Etcher (https://www.balena.io/etcher/).
- Launch the program, select the downloaded .img file, select the target USB drive, and execute the "Flash" option. Remove the USB device when finished.

Next, the following steps install pfSense to the Protectli Vault.

- Verify that the new hardware is powered down.
- Verify that a monitor and USB keyboard are connected directly to the Vault.
- Insert the USB install drive into another USB port on the hardware.
- Power the device and verify that it boots and begins the installation process.

If your Vault does not recognize the USB device and cannot boot into an operating system, you must enter the BIOS of the device and configure it to boot from USB. The procedure for this is different on any machine, but the Protectli Vault is fairly straight-forward.

- Turn on the device and immediately press F11 on the keyboard repeatedly.
- If the USB device is visible on the monitor attached to the Vault, select it.
- If USB device is not visible, enter the setup menu and use the right keyboard arrow to highlight "Boot", use the down arrow to highlight "Hard drive priorities" change Boot Option # 1 to the USB drive, and strike "F4" to save and exit.

Remove the USB device when the firewall reboots. From there, follow all default installation options, which should require you to strike the enter key several times. After install, connect a computer via ethernet cable to the LAN port of the Protectli Vault. Navigate to 192.168.1.1 within a web browser and log in with the default username of "admin" and password of "pfsense". Some browsers may warn you about the lack of an SSL certificate. This is normal, and you may need to click "Advanced" in order to allow this "site" to load. Accept all defaults within the setup process with "Next". Be sure to create a very secure password on the final step of this process.

Phase Two: Activate Ports (Optional)

If you purchased a 4-port or 6-port option, you can activate these ports at this time by configuring the following changes. If you purchased the 2-port FW2B, skip this page.

- Navigate to "Interfaces" then "Assignments".
- Click the "Add" option next to each empty port, which will add one port at a time.
- Repeat until all ports have been added and "Add" is no longer available.
- Save your changes.
- Click through each new option (likely Opt1, Opt2, etc.).
- Enable each port by checking the first box, and saving your changes each time.
- When finished with all of them, apply the changes in the upper right.
- Navigate to "Interfaces", "Assignments", then select "Bridges" in the upper menu.
- Click "Add" to create a new bridge.
- Select the LAN option as well as each port that was added with ctrl-click or cmd-click.
- Provide a description as "bridge" and click "Save".
- Navigate to "Firewall" then "Rules".
- Click each port and click the "Add" button (up arrow) for each.
- Change the "Protocol" to "Any".
- Click "Save" after each port is modified.
- Apply changes in upper-right after all ports have been added.
- Navigate to "Interfaces" then "Assignments".
- Click "Add" next to "BRIDGE0" and click "Save".
- Click on the bridge, which may be labeled as "Opt(#)".
- Enable the interface and change the description to "bridge".
- Click "Save" and then "Apply Changes".
- Navigate to "Firewall" then "Rules".
- Click on "Bridge" then click the "Add" button (up arrow).
- Change the "Protocol" to "Any" and click "Save".
- Apply changes in upper-right.

Please note that enabling these ports allows you to attach additional devices to your firewall. However, you may need to have an active ethernet device plugged into the LAN port of the firewall in order for the additional ports to function. At this point, you should still have your primary computer plugged into the LAN port of the firewall. Once Wi-Fi is enabled, as explained later, you can remove this cable.

Phase Three: Disable IPv6

Connect your internet access (cable modem, DSL, etc.) to the WAN port of the pfSense device and reboot the router. It should now have internet access, visible in the Interfaces section of the Dashboard under WAN. It should display the IP address of your connection. This will be required in order to complete the next step. Note that you will be sharing your real IP address with any services until your VPN is configured. Therefore, I recommend connecting a VPN through your own computer as usual during this process.

IMPORTANT REMINDER: If you are installing this firewall at your new anonymous home, and you have never exposed your new devices to your true home IP address, do not connect a traditional Apple or Microsoft device to your firewall in order to complete the installation. A clean Linux machine will give you much more anonymity as it does not collect user information and send it to a data collection center. If you do not have a dedicated Linux device, use a live Linux boot USB environment. TAILS (explained later) is an easy option that will work with most machines.

Ultimately, we just do not want to have your Apple or Microsoft devices associate your new home IP with your new device accounts. If the Linux option is not available to you, do not connect your home internet to this device yet. If you have already connected your computer to your home internet connection in the past, there is no harm continuing this process without VPN protection.

One issue that I have found that conflicted with my test units was the presence of IPv6 IP addresses. Your ISP may require you to use IPv6, but I rarely find that to be the case. If disabling this prevents your internet connection from functioning, you may need to skip this step. I chose to completely disable IPv6 by conducting the following:

- Navigate to "Services" then "DHCPv6 Server".
- Un-check "Enable DHCPv6 server on interface LAN" and click "Save".
- Navigate to "Interfaces" then "LAN".
- Change the IPv6 configuration type to "None".
- Click "Save" and "Apply changes".
- Navigate to "Diagnostics" then "Reboot" to restart the router.
- Log in with your pfSense credentials.

Phase Four: VPN: Configure your VPN settings and account

Overall, pfSense is already a powerful firewall by default. It blocks some undesired incoming traffic through your internet provider and protects the devices within your home. My priority from there is to create a constant VPN on the device which possesses a "kill switch". This configuration ensures that I never expose my true IP address to any services or sites from any device in my home. Before proceeding, please note that pfSense configures your settings based on the hardware present. Each install can be unique, and your software version may appear slightly different than my tutorials. Please only consider this a general guide for configurations within your pfSense installation. I hope these examples are received as concepts rather than specific instructions which can be applied globally. However, many people have followed these exact steps in order to produce their own home firewall.

I present two options during this phase, but you should only complete one. In the first example, I demonstrate configuration of a Private Internet Access (PIA) VPN. This is almost identical to the tutorial from the previous edition of this book. Afterward, I present the exact steps if you choose ProtonVPN as your VPN provider. Each of these steps would be very similar if you chose yet a different VPN. I have widened the scope in this edition due to many people abandoning PIA for ProtonVPN.

It is vital to choose a stable VPN provider with good speed and reputable privacy policies. I discussed the pros and cons of these two providers previously, but let's take another look. PIA is more affordable and a bit easier to implement, but comes with the concerns about its recent acquisition by a larger parent company with a questionable past. ProtonVPN offers a higher level of privacy and security (in my opinion), but costs a bit more. It also requires a few extra steps during configuration. PIA is more popular, which makes you a smaller needle in a larger haystack. ProtonVPN has less users, which means less people associated with each IP address. This could lead to less restrictions on sites which block VPNs and fewer captchas when visiting websites with DDOS protections.

Either of these options provide broad protection from ISPs snooping on your traffic. PIA is an affordable "catch-all" U.S. solution, while ProtonVPN provides greater privacy from Switzerland without concerns of Five Eyes countries attempting to intercept traffic. PIA offers easier connections to randomly selected servers within a specific geographical location, while ProtonVPN demands that you choose a specific server IP address for all connections. This static IP address could slightly weaken your privacy strategy. PIA has no limitations for downloading large Torrent files, while ProtonVPN insists this activity is isolated to specific servers. Most users will see no difference in the usage of one provider versus the other. Near the end of this chapter, I present an option where you may require two VPNs and provide a summary of all choices. Please check **https://inteltechniques.com/vpn.html** for the latest information about suggested VPN providers. **Most clients' firewalls use PIA as the VPN**.

Phase Four (Option One): VPN (PIA)

These instructions assume you possess VPN service through PIA. First, download the CA certificate files at https://www.privateinternetaccess.com/openvpn/openvpn.zip. Unzip this file, locate the file titled "US West.ovpn", and open it with a standard text viewer such as TextEdit (Mac) or Notepad (Windows). Then, conduct the following steps.

- Log in to the pfSense device through your browser.
- Navigate to "System" > "Cert Manager" > "CAs".
- Click on "Add" in the lower-right and use the following details:
  Descriptive name: VPN
  Method: Import an existing Certificate Authority
  Certificate Data: Open "US West.ovpn" in a text editor and copy/paste the entire text from including "-----BEGIN CERTIFICATE-----" through "-----END CERTIFICATE-----"
  Certificate Private Key and Serial: Leave these blank
- Click "Save".
- Navigate to "VPN" > "OpenVPN" > "Clients".
- Click on "Add" in the lower-right and enter the following details:
  Server Mode: Peer to Peer (SSL/TLS)
  Protocol: UDP on IPv4 Only
  Device Mode: Tun - Layer 3 Tunnel Mode
  Interface: WAN
  Local Port: Empty
  Server Host or Address: (See details on next page)
  Server port: 1198
  Proxy host or address: Empty
  Proxy Port: Empty
  Description: Empty
- Under the "User Authentication" section, provide your PIA username and password.
- Under the "Cryptographic Settings" section, enter the following details:
  TLS Configuration: Ensure "Use a TLS Key" is disabled
  Peer Certificate Authority: Select the "VPN" option created earlier
  Client Certificate: None (Username and/or Password required)
  Encryption Algorithm: AES-128-CBC (128-bit)
  Auth digest algorithm: SHA1 (160-bit)
  Hardware Crypto: No Hardware Crypto Acceleration

- In the "Advanced Configuration" section, enter the following in "custom options":
  persist-key
  persist-tun
  remote-cert-tls server
  reneg-sec 0
- Click "Save".

Server Host or Address: Traditionally, you would choose an address from PIA's server website at www.privateinternetaccess.com/pages/network/. Examples of this would be an east coast server address of us-east.privateinternetaccess.com or a west coast server address of us-west.privateinternetaccess.com. Place the chosen option in the "Server Host or Address field". Always choose a server close to you if speed is a priority. Choosing a server far away from you may be appropriate if privacy is your biggest priority. This is also an opportunity to make all of the internet traffic from your home appear to be coming from a specific location. If you live in California, you could choose a Texas server. The pattern of location data collected by hundreds of online companies will display evidence you reside in Texas.

Now, let's test our VPN connectivity.

- Navigate to "Status" > "OpenVPN".

If Status doesn't show as "up", click the circular arrow icon under Actions to restart the service. If it still does not come up, navigate to "Diagnostics" > "Reboot" to restart the device. Ensure that "Status" shows as "up" before continuing. This means that your router is connected to your VPN provider. You should now have PIA masking your IP address from any sites you visit. We will test this later.

In my experience, the certificate data which was copied and pasted into pfSense is the same for all PIA servers. This can be quite convenient. You can now navigate to "VPN" > "OpenVPN" > "Clients" and edit this setting at any time. You can easily switch your entire network to another region or another country by simply changing the "Server Host or Address" field. I find the following servers to be most beneficial in addition to the two already previously presented.

us-california.privateinternetaccess.com
us-lasvegas.privateinternetaccess.com
us-chicago.privateinternetaccess.com
us-newyorkcity.privateinternetaccess.com
uk-london.privateinternetaccess.com
ca-toronto.privateinternetaccess.com
swiss.privateinternetaccess.com
de-berlin.privateinternetaccess.com

Phase Four (Option Two): VPN (ProtonVPN)

These instructions assume you possess VPN service through ProtonVPN. First, we need to download their certificate, which involves a few extra steps. Much of this tutorial is identical to the previous PIA example, but I include every step for accuracy. First, log in to your ProtonVPN account and navigate to https://account.protonvpn.com/downloads. Conduct the following steps.

- Under OpenVPN Configuration Files, select "Router".
- Under Protocol, select "UDP".
- Under Connection, select "Server Configs".
- Choose your desired country of VPN.
- Click the "Download" button next to your desired server and save the file.

The number of servers is a bit overwhelming. If you are a paid ProtonVPN user, I recommend servers that are marked with a "P". This indicates the server is only for use by "Plus" plans or higher. Servers marked with "Tor" or "Free" may be much slower. Free users can take advantage of some servers, but expect slow speeds. After you confirm you can access the content within the downloaded file, conduct the following steps.

- Open the pfSense dashboard through your web browser.
- Navigate to "System" > "Cert Manager" > "CAs".
- Click on "Add" to add a new certificate and use the following details:
  Descriptive name: VPN
  Method: Import an existing Certificate Authority
  Certificate Data: Open the downloaded certificate in a text editor and copy/paste the text from "----BEGIN CERTIFICATE-----" through "-----END CERTIFICATE-----"
- Click "Save" and navigate to "VPN" > "OpenVPN" > "Clients"
- Click on "Add" in the lower-right and enter the following details:
  Server Mode: Peer to Peer (SSL/TLS)
  Protocol: UDP on IPv4 Only
  Device Mode: Tun - Layer 3 Tunnel Mode
  Interface: WAN
  Local Port: Empty
  Server Host or Address: (See details on the next page)
  Server port: 1194
  Proxy host or address: Empty
  Proxy Port: Empty
  Description: Empty

- Under "User Authentication Settings", provide your ProtonVPN "OpenVPN / IKEv2 username" username and password available in the "Account" of your ProtonVPN online dashboard. This may be different than your credentials to log in to ProtonVPN.
- Under the "Cryptographic Settings" section, enter the following details:
  TLS Configuration: Ensure "Use a TLS Key" is enabled.
  Automatically generate a TLS Key: Ensure this is unchecked.
  TLS Key: Open the downloaded certificate in a text editor and copy/paste the text beginning with "-----BEGIN OpenVPN Static key V1----" and ending with "-----END OpenVPN Static key V1-----".
  TLS Key Usage Mode: Ensure "TLS Authentication" is selected.
  Peer Certificate Authority: Select the "VPN" option created earlier.
  Client Certificate: None (Username and/or Password required)
  Encryption Algorithm: Select "AES-256-CBC (256 bit key, 128 bit block)".
  Enable NCP: Ensure this is checked.
  Auth digest algorithm: Select "SHA512 (512-bit)".
  Hardware Crypto: Select "No Hardware Crypto Acceleration".
- Under "Tunnel Settings", enter the following details within "Custom Options":
  Compression: Select "LZO Compression [compress lzo…]".
  Topology: Select "Subnet — One IP address per client in a common subnet".
  Don't pull routes: Ensure this is checked.
- Under "Advanced Configuration", enter the following within "Custom Options":
  tun-mtu 1500;
  tun-mtu-extra 32;
  mssfix 1450;
  persist-key;
  persist-tun;
  reneg-sec 0;
  remote-cert-tls server;
  pull;
- Ensure "UDP Fast I/O" is checked.
- Ensure "Send/Receive Buffer" is set to "Default".
- Ensure "Verbosity level" is set to "3 (recommended)" and click "Save".

Server Host or Address: This is a bit trickier than the PIA setup. We must choose a server, translate the server name to an IP address, and populate that data. If that specific server IP address should change or become overloaded, our firewall will not function. We would need to repeat the process to find a new server. This is one advantage of PIA over ProtonVPN. With PIA, we chose a server farm and allowed PIA to choose the best server each time we boot the firewall. ProtonVPN requires more specific data. I chose "US-TX#1" from the list

previously mentioned. Next, I navigated to https://mxtoolbox.com/DNSLookup.aspx. I entered the proper structure for the chosen server (us-tx-01.protonvpn.com), which produced a result of 209.58.147.42. I placed this IP address in the "Server Host" field. My firewall will connect to this server each time. If you have no preference of a specific location, such as a nearby state, **you can simply enter a country domain, such as us.protonvpn.com, in the "Server Host" field**. This will always connect to the fastest server in the country. Let's test!

- Navigate to "Status" > "OpenVPN".

If Status doesn't show as "up", click the circular arrow icon under "Actions" to restart the service. If it still does not come up, navigate to "Diagnostics" > "Reboot" to restart the device. Ensure that Status shows as "up" before continuing. This means that your router is connected to your internet connection and is protected by your VPN provider. You should now have ProtonVPN masking your IP address from any sites you visit. We will test this later.

I noted previously that ProtonVPN only allows torrent downloads from specific servers. These server details can change at any time. When you are using their VPN application, it simply switches you to another server if a torrent download begins. With a firewall connected to a specific IP address, we do not have that luxury. If you do not know what torrent files are, then you have nothing to worry about. If you know that you need this ability, make sure you select a "Pro" server from the list.

At the time of this writing, the following servers could be used within this configuration, with the corresponding IP addresses for entry into pfSense. Each of these allow access through both "Basic" and "Pro" plans. All should allow torrenting.

US-California: 209.58.129.97
US-Utah: 173.231.63.98
US-Texas: 209.58.147.42
US-NYC: 69.10.63.243
US-Florida: 37.120.215.243
Canada: 104.254.92.59
Switzerland: 185.159.157.19

If desired, you can add multiple servers under the "Advanced Configuration" option explained in the previous page (directly under "pull;"). This will issue a random server upon boot and skip any server which does not respond. The following text adds two Texas options to our existing configuration. This way, we have a total of three Texas servers available to us without modifying pfSense whenever a server is unavailable. This provides great redundancy since ProtonVPN does not support domain-based server selection.

```
remote 209.58.147.43 1194;
remote 209.58.147.44 1194;
remote-random;
```

Phase Five: Routing: Properly route all internet traffic

Next, we want to add the new VPN which we created as an interface.

- Select "Interfaces" and click "Assignments".
- Select "ovpnc" from the bottom option.
- Click "Add", then click "Save".

Notice the name assigned, as it may be similar to OPT2 or OPT5. Click on this new name, which should present the configuration for this interface.

- Enter the following under "General Configuration":
  Enable: Check this box
  Description: OVPNC
- Click "Save", then "Apply changes".
- Navigate to "Firewall" > "NAT".
- Click on "Outbound" at the top.
- For "Outbound NAT Mode," select "Manual Outbound NAT rule generation".
- Click "Save" then "Apply Changes".
- In the lower portion of the screen, click the pencil icon (edit) next to the option with a description similar to "Auto created rule - LAN to WAN".
- Change the "Interface" option of "WAN" to "OVPNC" and click "Save".
- In the lower portion of the screen, click the pencil icon (edit) next to the option with a description similar to "Auto created rule for ISAKMP - LAN to WAN".
- Change the "Interface" option of "WAN" to "OVPNC" and click "Save".
- Click "Save" then "Apply Changes".

This phase tells your firewall to route the internet traffic from your various devices through the VPN which you configured on the firewall. This ensures that all of your devices ONLY connect through a VPN, and eliminates the need to possess a VPN connection on a specific device itself. This is vital for hardware which cannot host a VPN connection, such as streaming devices, IoT units, and e-book readers. However, if your VPN fails, you will be exposed. Because of this, we will execute the next phase in order to kill your entire internet connection if the VPN is not protecting your network.

Phase Six: Kill Switch to prevent internet access unless routed through VPN

Your firewall should now automatically connect to PIA or Proton VPN upon boot. This means all of your internet traffic from any device within your home is now protected. However, VPN connections are known to fail, reset, or otherwise leave the user exposed. I believe that no website or online service should ever know your real IP address, and I cannot take the chance of exposure. Therefore, we should make the following changes in order to protect from leakage. Some of this may appear redundant on your installation, but I will verify all of these settings to ensure your device is protected.

- Navigate to "Firewall" > "Rules" > "LAN".
- Click the pencil icon (edit) next to the option with a description of "Default allow LAN to any rule".
- Click the "Display Advanced" option near the bottom.
- Change the "Gateway" to "OVPNC_VPNV4".
- Click "Save" then "Apply Changes".
- Click the pencil icon (edit) next to the option with a description of "Default allow LAN IPv6 to any rule".
- Change the "Action" setting from "Pass" to "Block".
- Click "Save" then "Apply Changes".

This configuration should harden your network and protect you if your VPN should ever fail. It is vital to test this, which will be explained soon. Remember this whenever your internet "goes out". If your firewall is on at all times, I suspect you will experience outages when the VPN disconnects. Since I turn my firewall and internet connection completely off every night, I rarely experience outages during the day and evening when it is active.

If your internet connection is ever unavailable because of a VPN disconnection, you can still open your browser and connect to the firewall at 192.168.1.1. From within the pfSense menu, you can select "Status" > "OpenVPN". Clicking the circle with a square inside, on the far right, stops the VPN server. Clicking the triangle in this same location starts the service. In my experience, this repairs any outage due to a failed VPN connection. I highly recommend becoming familiar with this process, as you will not have an internet connection to research issues if there is a problem. If desperate, shutting down the device and turning it back on often resolves issues with a failed VPN connection. **Pressing the power button (quick press) on a running Protectli Vault shuts the pfSense process down properly.** Pressing it again reboots the device. **Never hold the power button down longer than a second unless your device is locked-up or not responsive.**

Phase Seven: DNS Servers: Prevent DNS leakage

The previous steps force the firewall to use your VPN interface as the default gateway. This means only the VPN can serve web pages, and not the raw internet connection delivering internet access to the device. However, your ISP's DNS servers are possibly still being used. DNS is the technology which translates domain names into the IP addresses needed to complete the connection. Using the default DNS servers from your ISP would tell your ISP every website that you visit, but they could not see the content. It is possible that your VPN provider is acting as a DNS server, which may be acceptable.

Personally, I choose to use a third-party DNS provider in order to have another layer of privacy. My VPN provider is providing my internet access and content, but a third-party DNS can look up the requests to provide the content to the VPN. This takes away a bit of knowledge about my internet browsing from the VPN company, but not much. Since we are seeking extreme privacy, I believe this extra step is justified. Choosing an alternative DNS provider will also allow us to encrypt our DNS traffic. Many DNS providers do not allow encrypted connections, so I will use one that does. I chose to make Cloudflare my firewall DNS provider. They are not perfect, and have financial motives for their huge company, but they are better than most of the alternatives, such as Google. I chose Cloudflare because they are one of the few DNS providers which provide encrypted DNS, promise to destroy connection logs after 24 hours, and has been independently audited by KPMG.

Navigate to the Dashboard by clicking the pfSense logo in the upper left. You will likely see your real ISP or VPN DNS servers listed under "DNS Server(s)". Conduct the following to change this.

- Navigate to "System" > "General Setup".
- Delete any DNS Servers specified.
- Ensure "Allow DNS server list to be overridden" is NOT checked.
- Ensure "Do not use the DNS Forwarder/DNS Resolver…" is checked.
- Add the following DNS servers and choose the "WAN_DHCP-wan" interface:
  1.1.1.1
  1.0.0.1
- Save the settings, and reboot the router.
- Return to the Dashboard and ensure that the only DNS servers listed are those above.
- Navigate to whatismyipaddress.com and ensure that your VPN IP address is shown.
- Conduct an Extended Test at dnsleaktest.com and ensure that only the chosen DNS provider details are shown.

You may notice that your VPN provider is still acting as your DNS server. This is common and is likely a service to protect you from your own ISP eavesdropping on your traffic. However, I insist on the third-party option. In order to truly force pfSense to allow the third-party DNS and not rely back on the VPN provider, we can force DNS encryption over TLS.

- Navigate to "Services" > "DNS Resolver" > "General Settings".
- Check the "Enable DNS Resolver" option.
- Uncheck the box under "DNS Query Forwarding".
- Add the following under Custom Options (if using Cloudflare):

```
server:
forward-zone:
name: "."
forward-ssl-upstream: yes
forward-addr: 1.1.1.1@853
forward-addr: 1.0.0.1@853
```

- Click "Save" then "Apply Changes".

Why is this important? If you have configured your firewall correctly, all DNS requests from your devices will be handled by Cloudflare. By enabling DNS over TLS, the requests are encrypted and your ISP will only see that you are connecting to a DNS provider without being able to see the requests themselves. In other words, your ISP will not know which websites you visit, only the amount of data used to generate the content.

There are many DNS server options. While I chose to use Cloudflare, you could easily pick another option such as OpenDNS. I chose Cloudflare in order to take advantage of the encrypted option and eliminate any extra potential data leaks. Many VPNs use their own DNS servers, but some leak to your internet service provider. The most vital concern here is to occasionally test for DNS leaks at dnsleaktest.com. Overall, I do not like placing all of my eggs (visited websites) in one basket (VPN provider). Isolating these tasks provides another layer of privacy and security. If you would like more information about DNS as it relates to privacy, please listen to my podcast on this topic titled, "124-Does DNS Matter?" on my website at **https://inteltechniques.com/podcast.html**.

Do not take the choice of VPN and DNS providers lightly. Do your homework and make the best decision for your needs.

Phase Eight: Disable Annoyances and Test Device

You may have a hardware device with an internal speaker. If so, you may choose to disable the audible alerts presented at boot and shutdown. Conduct the following to eliminate these noises.

- Navigate to "System" > "Advanced" > "Notifications".
- In the "Sounds" section, check the "Disable startup/shutdown beep" option.
- Click "Save".

You should now test your new "kill switch". If you have not yet connected your internet access due to fear of exposing your true IP address to your Mac or Windows computer, you must make a decision now. Either you find a Linux machine for testing (preferred), or you cross your fingers and hope it all works. If you have previously been using unprotected internet in this home, there is no harm connecting internet access to this device. After selecting the most appropriate option for your threat model, connect your internet connection to the WAN port of the Vault and verify you have an internet connection within a web browser.

Navigate to "Status" > "OpenVPN" and click the small square "Stop OpenVPN" Service button to the right of the interface. Once it is stopped, try to connect to any website within your browser. You should receive a notification that you cannot connect. This means that without the VPN properly running, you have no internet access. Reboot your device to return to a protected state. Conduct a final test on the following websites and make sure that your IP address and DNS server addresses match with what you chose during the setup.

https://www.dnsleaktest.com/
https://browserleaks.com/ip
https://www.deviceinfo.me/

I also strongly recommend attaching an uninterruptable power supply (UPS) between the firewall and power source. Protectli offers an affordable small version designed for use with their devices. If power should be eliminated while the device is functioning, it can cause a corruption in the operating system which could prevent rebooting. This would leave you stranded without internet. Be sure to always power the device down completely before disconnecting from a power supply.

Let's pause now and reflect on what we have achieved. The pfSense firewall is providing protection between your internet connection and your laptop, which is likely still connected to the LAN port of the firewall. The VPN within the firewall makes sure that your laptop never sends data from your true IP address. If you never plan to connect other devices, such as a wireless router, tablet, or streaming service, then your setup may be finished. This would

be a rare scenario. In a moment, I explain how to introduce Wi-Fi to this configuration. The DNS servers that translate domain names into IP addresses are only those associated with a third-party DNS provider with a strong privacy policy. Overall, this means you will never expose your internet history to your internet service provider.

Many readers may be questioning the need to do all of this when we could simply use a VPN application on each of our devices. Consider one more example. You are at home and your wireless router is connected directly to your home internet connection without a firewall. The router is using your real IP address assigned by your provider. You boot your Windows or Mac laptop, and a connection to the router is made.

In milliseconds, your computer now has full internet access using your real IP address. Windows computers will start to send data to Microsoft while Mac computers will begin synching with Apple. This will all happen in the few seconds in between establishing internet access and your software-based VPN application on your computer connecting to the secure tunnel. In that brief moment, you have told either Apple or Microsoft who you really are and where you live. Both store these IP addresses for a long time, possibly forever. With a firewall solution, this does not happen.

Once you have your device exactly as you like it, navigate to "Diagnostics" > "Backup & Restore". Create a backup of all of your configurations and store in a safe place. If your system should ever become corrupt, or you make a change you cannot reverse, you can use this same option to restore from this backup file. If you make a mistake and simply want to start the entire process over, which I have needed to do several times, navigate to "Diagnostics" > "Factory Defaults" and reset everything. Be sure to check your dashboard on occasion and apply any updates from pfSense.

Finally, one last thing to consider. If you are setting up a new pfSense hardware device, the MAC address of the WAN port has never been used. This unique address will be shared with your internet service provider, which is not a big deal at this point. However, if you were to move to a new home, and take this device with you, the next internet service provider will see this same address. If you have the same provider, it would immediately know that you are the same customer, regardless of the name you provided for this new account. The solution is to either buy a new box when you move, or "spoof" the MAC address with the following steps.

- Navigate to "Interfaces" > "WAN".
- Provide a random set of numbers matching the pattern provided.

This should be done before connecting the internet connection. This may be overkill for some, but I want you to know your options and risks. Finally, let's simplify this entire process a bit.

Custom Configuration Scripts and Discounted Purchase Options

When I was updating this chapter for this new edition, I reached out to Brent from Protectli in order to have him test my settings and tell me where I was wrong. During our conversations, we discussed our concerns about offering highly technical tutorials to a mass audience. Both of us have heard from frustrated readers when a required step did not function as intended and served as a roadblock to the remaining instructions. We were also bombarded with questions about the appropriate models and hardware configurations. We decided it would be best to offer two things to all readers in order to eliminate some of the pain.

First, I have made several custom configuration scripts which can be imported into your own pfSense installation. These scripts contain the exact configurations presented in this chapter up to this point without much manual effort. Each script contains the appropriate VPN settings for U.S. east coast and west coast servers for both ProtonVPN and PIA. Full details, including direct download links and complete import tutorials can be found at **https://inteltechniques.com/firewall**. My recommendation is that readers understand the tutorials presented here and apply the modifications manually. This helps you understand the process. However, I do not want to exclude non tech-savvy readers from this amazing strategy. Possessing a firewall within your home network, even without fully understanding the technical details, is better than no protection at all.

Next, Brent has created a special page on his own site which limits the purchase options to only the recommended devices which are explained here. Personally, I recommend the 4-port or 6-port option (6-port if you have internet speeds over 250Mbps). Furthermore, he has included a small discount for readers. This is NOT an affiliate page. I receive no commission or kickback from your purchase, nor any details about you or your order. This link can be found at **https://inteltechniques.com/firewall**.

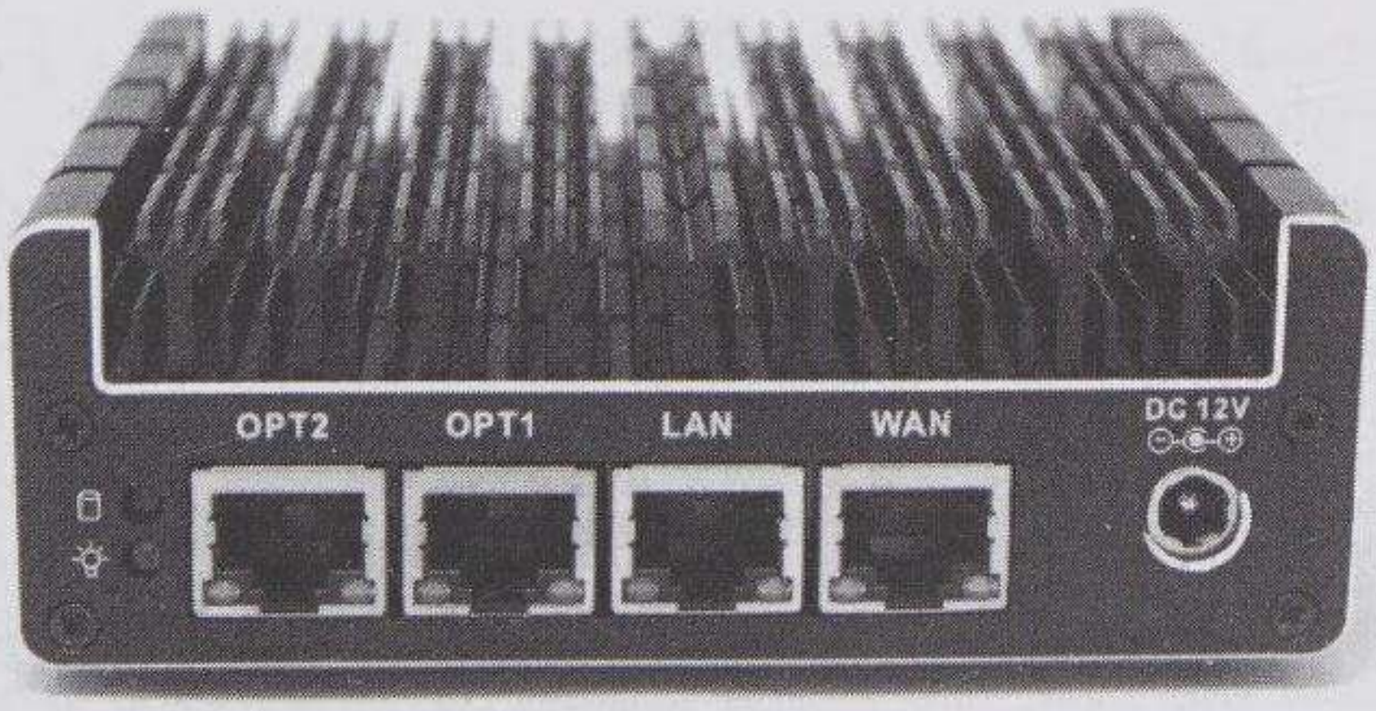


Figure 10.01: The Protectli Vault FW4B 4-port firewall.

Optional: Install pfBlockerNG

Prior to 2020, I included a "Pi-hole" within my home network. This small device is a Linux network-level advertisement and internet tracker blocking application, intended for use on a private network. Basically, it is a small box placed between my internet connection and my firewall in order to prevent undesired advertising content from being delivered to my devices. While I believe that Pi-holes are still great for home networks, I have transitioned to pfBlockerNG. This software can be installed directly within your pfSense installation, which eliminates the need for another piece of hardware within your network. The following steps configure this option within your current pfSense build.

- From the pfSense portal, click on "System" then "Package Manager".
- Click "Available Packages" and search for "pfBlockerNG".
- Click "Install" next to the "pfBlockerNG-devel" option.
- Click "Confirm" and allow the process to complete.
- When finished, click "Firewall" then "pfBlockerNG".
- Click "Next" until you are presented with "Component Configuration".
- Choose "WAN" for "Inbound" and "LAN" for "Outbound", then click "Next".
- Accept the default webserver configuration, click "Next", then "Finish".
- Allow the next page to complete the script download process.
- When complete, click the blue "Run" button in order to update all scripts.

You now possess basic pfBlockerNG protection from invasive ads and tracking. Combined with uBlock Origin, as previously explained, you have a great layer of privacy in both your network and your browser. There are numerous optional block feeds which can be enabled. The only additional configuration which I added was BBcan177, as explained below.

- Click "Firewall" then "pfBlockerNG" and select "Feeds".
- Find the "BBcan177" entry under the "DNSBL" section.
- Click the blue plus sign to the right of it.
- Click the blue "Enable All" button, then the "Save DNSBL Settings" button.
- Click the "DNSBL" menu link, then "DNSBL Groups".
- Change the BBcan177 setting to "Unbound" and click "Save".
- Click the "Update" menu item then the blue "Run" button.

The home page of the portal should now display a new section in the lower right. This window presents statistics regarding the number of intrusions blocked. Navigate to a website such as Yahoo.com. You should see several white boxes in the place of advertisements. This confirms that your configuration is working.

Optional: Enable AES-NI CPU Crypto & PowerD

Prior to late 2019, pfSense insisted that version 2.5 of the firewall software would absolutely require an AES-NI cryptographic accelerator module. The company has since stated that it will not be mandated (for now). However, we should always future-proof our devices whenever possible. The Protectli Vault firewall supports this feature, which is disabled by default on any pfSense installation. Before I explain the process to activate this setting, we should first understand the technology.

A cryptographic accelerator module uses hardware support to speed up some cryptographic functions on systems which have the chip. AES-NI (AES New Instructions) is a new encryption instruction set, available in the firewall processor, which speeds up cryptography tasks such as encryption/decryption for services such as OpenVPN. In other words, it might make your firewall traffic faster. In my experiences, it did not change much. However, I believe you should consider activating the feature now in order to be prepared whenever it is mandated. The following steps enable AES-NI within the pfSense firewall.

- From the pfSense portal, click on "System" then "Advanced".
- Click the "Miscellaneous" tab.
- Scroll to the "Cryptographic & Thermal Hardware" section.
- Select "AES-NI CPU-based Acceleration" in the drop-down menu.

Navigate back to the pfSense Dashboard and verify this new setting. Within the "CPU Type" section, you should see "AES-NI CPU Crypto: Yes (active)". Next, consider enabling "PowerD". This utility monitors the system state and sets various power control options accordingly. In other words, it can lower the power requirements whenever the firewall is in a state which does not demand high power. Navigate to the following to activate this setting.

System > Advanced > Miscellaneous > Power Savings > Enable "PowerD"

Please note that the configuration files hosted on my site which were previously mentioned already include the activation of AES-NI, but not the installation of pfBlockerNG or activation of PowerD. The advertisement blocking features of pfBlocker and custom power settings of PowerD may not be appropriate for all devices. Furthermore, this customization should always be manually applied in the event of a backup file restoration. I have witnessed several configuration files which include pfBlocker fail to load everything properly when used as an imported configuration. Overall, manually configuring everything in this chapter whenever possible is best. However, backup scripts may save you time when you need immediate access to the internet and your installation has become corrupt. Know all of your options, and understand the technology which makes everything function.

VPN Provider Options

You may still be questioning my recommendations of PIA or ProtonVPN as your VPN providers. For the record, I do not completely trust ANY VPN provider and no VPN is perfect. None of us know what is truly happening behind the scenes. Providers can promise "No Logging" policies, which would prevent them from disclosing your true IP address if provided a court order, but we really have no way of proving it. The following final summary may help you choose the provider best for your needs.

Cost: PIA is under $40 a year with access on up to ten devices. This is much lower than other reputable VPNs. While cost should never be a deciding factor when it comes to privacy and security, the low price helps me convince others to use a VPN at all times. Currently, ProtonVPN costs $53 annually for their "Lite" plan. This is still very affordable.

Court Orders: Reputable VPNs claim that they do not log users' IP addresses. We place a lot of trust in our VPN providers, and they rarely provide any proof to their anonymity claims. In 2016, search warrants issued by the FBI to PIA became public record. Basically, criminals were hiding behind PIA IP addresses, and the FBI came knocking to identify the suspects. While PIA cooperated, they simply had no data to offer. They did not have any logs which would identify the culprits. While I do not like that criminals escaped prosecution, it provides more confidence in my usage of the VPN service. I will always evaluate techniques used by criminals in order to provide my own personal protection while online. ProtonVPN will only respond to a Swiss court order, but still cannot provide logs in order to identify usage.

Servers: As stated previously, PIA chooses the best server in a specific area upon each boot. This means that my firewall is receiving a different IP address every time I restart it, which prevents me from always using the same exact IP address. ProtonVPN will use the same IP address every time unless I change it manually. This can be beneficial if you need to connect to a website or service from a whitelisted IP address, but that scenario is rare. Since we are using our pfSense firewall as the software, we are not relying on the PIA or ProtonVPN applications to protect us. If either were to embed any undesired software in their applications, it would not carry over to our firewall. Again, this is overly cautious, but this is extreme privacy.

Configuration: The PIA tutorial has been the most successful for readers. When I have walked people through the process for ProtonVPN, I have witnessed minor complications. Fortunately, ProtonVPN keeps an updated web page with an updated complete tutorial at https://protonvpn.com/support/pfsense-vpn-setup if anything should change.

I still rely on PIA for most home firewalls, but insist on the ProtonVPN app while traveling and any time there is a need for a secondary VPN, as explained next. EITHER can work as your only VPN option for personal devices and a firewall.

Secondary VPN

When I am at home on my VPN protected firewall, I do not need a VPN application on my devices. However, I still possess a secondary VPN option for extreme scenarios. Since I often use PIA on the firewall for fast catch-all VPN coverage, I choose a different provider on my devices. Currently, I rely on ProtonVPN when I need secondary protection due to sensitive investigations. Recent news about the feuds between PIA and ProtonVPN has made it clear that these two companies are competitors. That makes me suspect they are not owned by the same company. Many VPN providers are simply resellers for another service. I do not believe that to be the case here. If I am protected by both services, I have an even smaller chance of my true ISP-provided IP address being associated with my internet traffic.

PIA is a company with strong ties to the U.S. and the U.K. (Five Eyes countries), which can be a deal breaker for some privacy enthusiasts. However, it might be desired by American users with adversaries overseas. I prefer PIA on my firewall as I want to be an extremely small needle in a very large haystack. PIA is very popular and has more users than most VPNs. ProtonVPN has a smaller user base, and they are headquartered in Switzerland (not a Five or Fourteen Eyes country). I may blend in better with PIA, but possess better protection from U.S. entities by using ProtonVPN.

Any time I am conducting any type of extremely sensitive internet usage, I am behind two VPNs. The firewall (PIA) is the first layer which is masking my true IP address throughout my entire home network, and the VPN app on my device (ProtonVPN) is the second layer that routes my traffic through another country (when a foreign server is chosen). The chances of both services failing or sharing my true information is extremely slim. Regardless, I purchase each anonymously with prepaid cards obtained with cash.

Is this overkill? Probably. Do you need this redundant setup? I doubt it. However, if you are worried that a failure of one VPN could expose you or your investigation, then it is worth it to double-up. If you really want to go the distance, run PIA on your firewall, ProtonVPN on your devices, and the Tor Browser as your window to the internet (more on this later). Expect your internet speed to slow to a crawl. Overall, most readers would never need a secondary VPN if you have a properly configured firewall.

As a final reminder, I often update my list of recommended VPN providers and any related conversation on my website at **https://inteltechniques.com/vpn.html**. I also offer affiliate links for purchase at discounted rates on this page.

Wireless Router

This pfSense setup is missing one major feature. There is no Wi-Fi. After you have built your home firewall, you can associate it with any wireless router by connecting an ethernet cable from the LAN port of the firewall to a port on the wireless router. Be sure to disable DHCP, DNS, and any firewall settings within the wireless router's options as to avoid conflicts. Be sure that you are only running a VPN on the pfSense device as to not suffer performance issues. In a moment, I offer a simpler Wi-Fi solution for pfSense users. First, you should question whether you need wireless access at all.

The majority of my work is conducted on a laptop with an ethernet connection directly to my firewall. Wireless access is not required for this. I leave my Wi-Fi device off most of the time when I am working. However, I often need Wi-Fi for my mobile device, especially since I do not allow a cellular connection from my home. It is also unrealistic to think that the other occupants of your home will go without Wi-Fi.

By possessing separate devices for your internet connection (cable modem), firewall (pfSense), and wireless router (Wi-Fi), you can control the ability to disable them as needed. As an example, my ISP provided modem is always on. The firewall is on during the day, but I shut it down at night when it is not needed. The Wi-Fi is only on when needed, but not necessary for internet connection to my laptop. This may seem all overboard, but the ability to disable my Wi-Fi is important to me. The following may help explain why.

Most homes have wireless internet access. This involves at least one wireless router which is connected to your internet access provider via a modem. If you purchased your own wireless router, it mandated some type of setup upon installation. This likely included a default name of the router which you may have customized. If the default was accepted, your router may have a name such as Netgear or Linksys (the brand of the router). While this is not best practice for security reasons, it does not violate much in the way of privacy. If you customized the name of the router, which is extremely common, it may be broadcasting sensitive details such as your family name. You can see the wireless network name on any device which you have connected such as a phone or laptop. If the network broadcasts a name that jeopardizes your privacy, change it to something generic according to the steps in the instruction manual.

Regardless of your current scenario, you should consider hiding your wireless network name, officially known as the SSID. Entering your setup utility on the wireless router from a computer connected to the device will allow you to change the broadcast setting to a hidden network. Again, seek the specific instructions for your router online or within the manual. Note that this does not make you invisible. There are plenty of tools which will identify hidden networks. However, this is not common activity conducted by your average neighbor. This will require you to know the specifics of your router when configuring new wireless devices

to access your network. The security and privacy benefits of a hidden network outweigh these rare configuration annoyances.

The biggest risk with a unique Wi-Fi network name is the collection of that information from services such as Google and Wigle. That bright Google street view car that takes photos of your home and then posts them to the internet for the world to view is also collecting your wireless network name for cataloging. Please pause a moment to consider the significance of this activity. If your home router is named "Bazzell Family", and Google or Wigle has collected this data, you are a search away from disclosing your true identity as associated with your home address.

There is a way to opt-out of this collection behavior, but it is not perfect. Some people have reported that the following technique is often successful, but not always. The premise is that you can add specific characters to your Wi-Fi network name which will prevent various collection services from acquiring your router's information. Google mandates that "_nomap" appear at the end of your network name while Microsoft requires "_optout" to appear anywhere within the network name. Therefore, a router name of "wifi_optout_nomap" would tell both services to ignore this router and not to display it within router location databases. Wigle accepts both of these options; therefore, this network name would be sufficient.

Choosing a Wireless Router

Ideally, you will possess a wireless router which supports open source firmware. Before jumping into options, we should consider the reasons this is important. When you purchase a typical Linksys, Netgear, Asus, or other popular router, it is pre-configured with proprietary software made by the manufacturer. Most people rarely access this firmware, and simply accept the default options. The router just "works" right out of the box. We should be concerned with the software which controls our devices. Most wireless routers possess two threats within this software.

The first is privacy. Most popular routers send usage metrics back to the manufacturer. These do not identify you by name, but may include enough details to identify your interests, general location, and internet service. Since your router has full internet access, it can send and receive as much data to and from the manufacturer as requested. At the very least, the manufacturer receives your IP address whenever it is queried.

Next is security. Manufacturers want to present a smooth experience without technical complications. In order to achieve this, routers commonly have many unnecessary features enabled, including open ports which may present vulnerabilities. Furthermore, many manufacturers are slow to provide security patches once an issue is identified. Even if an update is available, few people apply any patches.

One solution to both of these issues is to "flash" your router with open-source software. This was explained briefly in my previous privacy books, but can quickly exceed the scope of this book. Overall, I recommend either OpenWRT or DD-WRT. Let's dissect each.

DD-WRT (https://dd-wrt.com): For most clients, I configure a Wi-Fi router with DD-WRT as the operating system. I first identify a router which is supported by DD-WRT. These include most versions of the Netgear Nighthawk R7000 AC1900, Linksys WRT3200ACM AC3200, and Asus RT-AC68U AC1900. These can all be found online and in stores. The DD-WRT website explains the process of replacing the stock firmware with this custom open-source software for each router.

OpenWRT (https://openwrt.org): This option is very similar to DD-WRT with a few important differences. Most importantly, there are fewer routers which support this operating system. While OpenWRT allows more granular control than DD-WRT, this can cause unnecessary confusion. This can be beneficial to some while a headache to others. I only recommend flashing your own router with OpenWRT if you have a deep understanding of networking and routers.

Tomato: In my previous privacy books, I had high praise for Tomato as the operating system for wireless routers. The specific builds I suggested are no longer updated. While there is still one Tomato project being updated, I no longer endorse it. The previous two options are superior in my opinion.

Whatever device you choose for your Wi-Fi needs, whether stock software or these custom options, remember to disable DHCP (assigns IP addresses) and place your Wi-Fi router into "Access Point" mode if available. If your Wi-Fi router is behind a pfSense firewall, the threat of privacy and security vulnerabilities is much less than if you did not have the firewall protection. Even stock routers without modification are fairly safe as long as they are behind the firewall. Choose the level of privacy and security most appropriate for your situation. The summary at the end of this chapter may help digest all of this information.

There are online providers which will sell you a router pre-configured with your choice of open-source firmware. However, the markup for this relatively easy service is high. I have seen router prices double when they include this free software. I strongly encourage you to research DD-WRT and OpenWRT, identify a supported router, and jump in. Learning the configuration process will help you maintain the device. Alternatively, you could consider a pre-configured "portable" router, such as the device mentioned in the next section. It should simplify all of this.

Portable Routers

A pfSense firewall is essential for a private and secure home, but can be overkill while on the road. However, blindly relying on public Wi-Fi is dangerous. You expose your current IP address (and location) at all times and could be vulnerable to malicious attacks from other devices on the network. This is where a travel router can be a vital piece of hardware for those commonly away from home. I currently provide a **Slate** (https://amzn.to/2FYo8i7) portable device to all of my clients who travel frequently, and some use it in their homes at all times as an access point. I explain two specific configurations within the following pages for these two scenarios.

This Slate portable Wi-Fi router is mighty for its size. The software is based on OpenWRT and possesses a menu system which is easy to navigate. There are many configurations, but I will focus on the most applicable to this book. First, let's assume that you want to use this as a Wi-Fi access point with a pfSense firewall. In this scenario, you created a pfSense unit which is connected directly to your home internet connection. You need Wi-Fi but do not want to self-install custom open-source software on a device. Since this is technically a travel router, the range will be less than a traditional unit. The following steps configure the Slate to be used as an access point with a pfSense firewall in your home.

- Power on the Slate device.
- Connect an ethernet cable from Slate WAN port to pfSense LAN port.
- Connect a computer or mobile device to the Slate via ethernet or Wi-Fi.
- Attempt to navigate to 192.168.8.1 within your browser.
- If the connection is allowed, skip to "Provide a new secure password" below.
- If the connection is refused, connect to the pfSense portal within your browser.
- Navigate to "Status" > "DHCP Leases" and identify the IP address of the Slate.
- Navigate to that IP address within your browser.
- Provide a new secure password.
- Under "Wireless" > "2.4G WiFi", click "Modify".
- Rename this SSID to something more private.
- Change the security password to something more secure and click "Apply".
- Repeat the process to rename and secure the "5G WiFi" option.
- Connect your computer's Wi-Fi to either SSID on the Slate.
- In the Slate portal, click on "Upgrade".
- If an upgrade exists, click "Download", then "Install".
- Click on "More Settings" > "Network Mode" > "Access Point" > "Apply".
- Reboot the Slate router, reconnect, test login, and ensure your VPN is active.

This is not the typical use for this router, but this scenario may help readers new to the idea of a firewall and router combination. The previous instructions place the router into "Access Point" mode which instructs it to provide Wi-Fi connections without controlling services such as assignment of IP addresses. It relies on the pfSense box to assign IP addresses, which is desired while at home. Basically, the Slate is acting as Wi-Fi only and passing the connections through to pfSense. Although it is not the most powerful or robust router out there, it has been the easiest for my clients to configure for use with pfSense in a short amount of time. Next, let's focus on the true intention of a portable router.

Assume you are at a hotel and need to access the public Wi-Fi. When you connect your laptop or mobile device, your VPN must be disabled in order to gain authorization through the hotel's login portal. Once you have internet connectivity, your device will begin to send numerous packets of data exposing your true IP address from the hotel. This traffic will also occur through the hotel's hostile network. Personally, I never connect any laptops or personal mobile devices directly through the hotel's Wi-Fi. Instead, I connect my travel router to the hotel network, and then connect all of my devices through the travel router. This allows me to possess unlimited devices on the network and all of them will be protected at all times by a single VPN connection. The following steps were conducted using a Slate router before and during travel, but could be replicated on practically any portable router using OpenWRT.

Before Travel:

- Power on the Slate device.
- Reset the Slate by holding the reset button for ten seconds and allowing reboot.
- Connect a computer or mobile device to the Slate via Wi-Fi.
- Navigate to 192.168.8.1 within your browser.
- Provide a new secure password.
- Under "Wireless" > "2.4G WiFi", click "Modify".
- Rename this SSID to something more private.
- Change the security password to something more secure.
- Click "Apply".
- Repeat the process to rename and secure the "5G WiFi" option.
- Connect your computer's Wi-Fi to either new SSID of the Slate.
- In the Slate portal, click on "Upgrade" > "Download" > "Install".
- Navigate to https://docs.gl-inet.com/en/3/app/openvpn/.
- Apply the appropriate VPN settings for your provider to the Slate.
- In the Slate portal, navigate to "VPN" then "VPN Policies".
- Click the "Enable VPN Policy" toggle and enable the remaining two toggles.
- In the Slate portal, navigate to "VPN" then "Internet Kill Switch".

- Enable the toggle option.
- Connect an ethernet cable from an internet connection to the Slate WAN port.
- Test internet and VPN connectivity through browser.

During Travel at Hotels with Ethernet Connections (Preferred):

- Connect a computer or mobile device to the Slate via ethernet or Wi-Fi.
- Connect hotel ethernet to the WAN port of router.
- Attempt connection to internet through a web browser.
- If presented a hotel login page, proceed through the process.
- Test internet and VPN connectivity through browser.

If your devices have VPN-protected Wi-Fi internet connectivity through the router, you are done. The portable router is providing the VPN service to anything connected. The hotel only sees one device (the router) and all data is traveling securely through the VPN. The ethernet connection is typically more stable than Wi-Fi, and I leave the device on for the duration of my stay. Unfortunately, hotel rooms with dedicated ethernet access is becoming rare. If your lodging only provides Wi-Fi, you can still make this strategy work for you.

During Travel at Hotels with Wi-Fi Connections:

- Connect a computer or mobile device to the Slate via ethernet or Wi-Fi.
- Navigate to 192.168.8.1 within your browser and log in to the Slate portal.
- Navigate to "Internet" and click "Scan" under "Repeater".
- Under "SSID" select the hotel's Wi-Fi network.
- If required, enter the password for the network.
- Click "Join".
- Attempt connection to internet through a web browser.
- If presented a hotel login page, proceed through the process.
- Test internet and VPN connectivity through browser.

If your devices have Wi-Fi internet connectivity through the Slate, you are done. I highly recommend leaving the router connected at all times in order to experience as few "dropouts" as possible. With both the ethernet and Wi-Fi options, you may be required to log in to the hotel portal daily during your stay.

Hotel Travel Router Troubleshooting

Since the router is trying to force usage of a VPN, the hotel's network may initially block the connection attempt. Many hotels demand that you first sign in to their own portal to verify that you are an active customer. The portal may refuse internet access to the router until this connection is authorized, which also prevents the VPN connection. Without the VPN connection, the router blocks all internet traffic. This can create a loop of failed requests. During a typical authorization process, the MAC address of a device is whitelisted in the hotel's network for the duration of your stay, and internet access is granted whenever requested. Since the router's MAC address is not authorized, we must "fake" it. During at least 50% of my hotel stays, the previous connection methods fail.

The following steps register a device with the hotel's network and clone that device's MAC address to the Slate router. I usually use my travel "burner" Android device for this process (which possesses the surveillance app Haven as previously explained), as I do not like to connect personal devices to hotel networks under any circumstance. I later explain how to create an Android mobile device which never sends data to Google.

- Connect to hotel Wi-Fi directly from a secondary (non-personal) mobile device.
- Authorize the connection through the hotel's Wi-Fi portal.
- Disconnect from hotel Wi-Fi and connect to the Slate travel router via Wi-Fi.
- Open the Slate portal (192.168.8.1) from a browser and log in.
- Navigate to "More Settings" then "MAC Clone".
- Identify the "Client" MAC address which represents your connected mobile device.
- Under "Your Router", select the MAC address of the mobile device.
- Click "Apply" and test internet and VPN connectivity through browser.

Let's pause a moment and digest these actions. The hotel's network is blocking the hardware MAC address of the Slate because it has not been registered. The hotel's network has allowed the MAC address of the mobile device since it was registered. Since we cloned the MAC address of the mobile device to the Slate router, the connection from the Slate to the hotel should be allowed. If required, you may need to repeat this process every 24 hours.

Some may read the previous section and question my trust of a third party (Slate) to modify open source software (OpenWRT) on a router. I understand this concern. After "sniffing" the Slate's packets of data, I found that it only made calls to time servers and an update server. This is very common for any open-source router. For those hardcore security readers, you could consider re-flashing the Slate to a pure version of OpenWRT. However, I do not recommend this unless you understand the risks and accept the security responsibilities. I believe the stock open-source software of the Slate is sufficient.

Firewall Troubleshooting

I have tested these configurations on numerous devices from various operating systems. I have found the following issues occasionally present within some installations.

ISP provided router: If your internet provider supplies you with a combination modem and wireless router, you may have IP address conflicts. The provided router will likely be using the IP scheme of 192.168.1.x which will cause a conflict from the beginning on your installation. The options to correct this situation are to either change the IP scheme in your provided router to something different (such as 192.168.9.x), or provide this new IP range to the pfSense installation. My preference is to change the IP address on your ISP provided router so that your pfSense device can be the primary network supplier. In this situation, you should also disable DHCP on the ISP provided router, and never plug any devices into that router. You would likely be unprotected by the VPN on pfSense. If your ISP provides a combination modem and Wi-Fi router, consider disabling the Wi-Fi feature completely. Connect the modem to the pfSense box, and then connect a wireless access point to the pfSense unit as previously discussed.

Updates: Minor updates to pfSense, such as 2.4.6 and 2.4.7 should not have a huge impact on your settings. However, major updates such as the upcoming 2.5.0 could have a large impact to your configuration. I originally created this tutorial on pfSense 2.3 and had to revisit every setting once I upgraded to 2.4, and again for this writing of 2.4.5. Therefore, be sure to back up all configuration settings before every upgrade. If necessary, you can always downgrade the software and reinstall your configuration file. As of versions newer than 2.5, pfSense will no longer work on devices which do not possess an AES-NI supported processor. Remember this when shopping for your device. You can identify your current version, and apply any updates, on the Dashboard page of your pfSense device.

VPN Blocking: Many video streaming services, such as Netflix, block all known VPN IP addresses in order to meet various location-based licensing restrictions. If you cannot access these services while behind your firewall, you will need to create a direct connection to your internet provider for that purpose. This action eliminates a big layer of privacy, but may prevent your family members from kicking you out of the house. I have one client who maintains a separate Slate router with an SSID of "Netflix". When the family wants to watch something, she plugs the internet directly into that router and connects the TV to it. There is no VPN protection, but also no personal devices being exposed within that network. This client must constantly choose whether the internet should be allocated to Neflix or everything else while protected with a VPN. Alternatively, you could program your 4-port or 6-port Protectli Vault to assign ports which do not possess any VPN protection. This also presents some risk, but eliminates the need to constantly switch connections. The following section explains the entire process.

Optional: The "Netflix" Port

This tutorial assumes that you have a 4-port or 6-port Vault, you have already completed the previous instructions including adding the additional ports, and you want to assign one of those ports to connect directly to your internet service provider without any VPN protection. This can be beneficial when you want to stream video from services such as Netflix, but the service is preventing the stream because they are blocking your VPN connection. The following steps reassign the last port on your device to remove the VPN, while still protecting the remaining ports including your Wi-Fi network on the LAN port.

- Within pfSense, navigate to "Interfaces" > "Assignments" > "Bridges".
- Click the pencil icon to edit the bridge.
- Hold the ctrl (or cmd) key and click to deselect the last port (similar to "opt5").
- Click "Save".
- Navigate to "Interfaces" > "Assignments".
- Click on the port which you just removed and configure the following:
  IPv4 Configuration: Static IPv4
  IPv4 Address: 192.168.2.1
  /: 24
- Click "Save" then "Apply Changes".
- Navigate to "Services" > "DHCP Server".
- Click the same port as previously mentioned.
- Select (check) the "Enable DHCP Server" option.
- Enter the range as "From: 192.168.2.100 To: 192.168.2.150".
- Click "Save".
- Navigate to "Firewall" > "NAT" > "Outbound".
- Click the first "Add" button.
- Change "Address Family" to "IPv4".
- Add a "Source Network" address of "192.168.2.0".
- Click "Save" and "Apply Changes".
- Navigate to "Firewall" > "Rules".
- Select the same target port as in the previous instructions.
- Click the pencil icon to edit the rule.
- Click "Display Advanced".
- Change the "Gateway" to "Wan…".
- Click "Save" then "Apply Changes".

The last port of the firewall should now connect directly through your ISP. This may be labeled OPT2 on a 4-port box or OPT4 on a 6-port box. Typically, it is the port to the far left when looking directly at the ethernet ports on the back of a Protectli Vault. Be careful with this! Anything plugged into that port has no VPN protection.

If you have a wired streaming device, you could plug it directly into this port in order to allow services such as Netflix to function. You lose a great layer of privacy here, as Netflix now knows your true home IP address. However, it also allows you to use their service and bypass their VPN restrictions. The remaining ports, including any Wi-Fi access point connected to your LAN port, still rely on a VPN. Anything connected to those ports are protected.

If desired, you could connect a Wi-Fi router to this newly configured port and allow streaming devices to connect wirelessly. You could replicate the same previous instructions with the Slate router and create a Wi-Fi network just for streaming. You would place the router into access point mode, connect an ethernet cable from the LAN port of the Wi-Fi router to the last port on the firewall, and change the SSID to something similar to "Netflix". Any device which connects wirelessly to this new network will not be protected by a VPN, but will allow access to all streaming services. Any time you encounter vital services which block VPNs, you would have an option which would allow the connection. Again, this increases your risk by exposing your true IP address to your ISP and the website or service used. If this strategy is executed, it should be used minimally.

If you have family members who demand to have unlimited access to services which commonly block VPNs, this can be a great technique. You can protect all of your personal online usage via a wired or Wi-Fi network through the LAN port of the firewall while being protected by a VPN. They can run their traffic through the second Wi-Fi network and bypass all of our privacy nonsense. Again, be very careful and deliberate here. Test everything twice before sharing with other household members. In a few pages, I present a diagram of how this might look within your home.

I would feel irresponsible if I closed this section without identifying my personal usage of this technique. Quite simply, I do not enable this feature. I believe exposing my true IP address to any service is too risky for my threat model. However, I also do not subscribe to services such as Netflix, Prime, or Hulu. All of these products monitor your viewing history, location, and schedule. The data is often shared with business partners and affiliates. When adding payment details, home address, and contact details, these services possess a powerful dossier about you.

The absence of streaming video within private homes can be a topic of heated debate between family members. If you lose this battle, know that you have an option which offers a compromise. Remember, privacy is best played as a long-game.

Optional: Embedded pfSense Wi-Fi

Protectli sells an optional Wi-Fi kit which is installed within the device before shipment. It presents an all-in-one firewall and Wi-Fi solution. However, the speeds are typically quite slow. The following steps configure pfSense if you possess an internal Wi-Fi device.

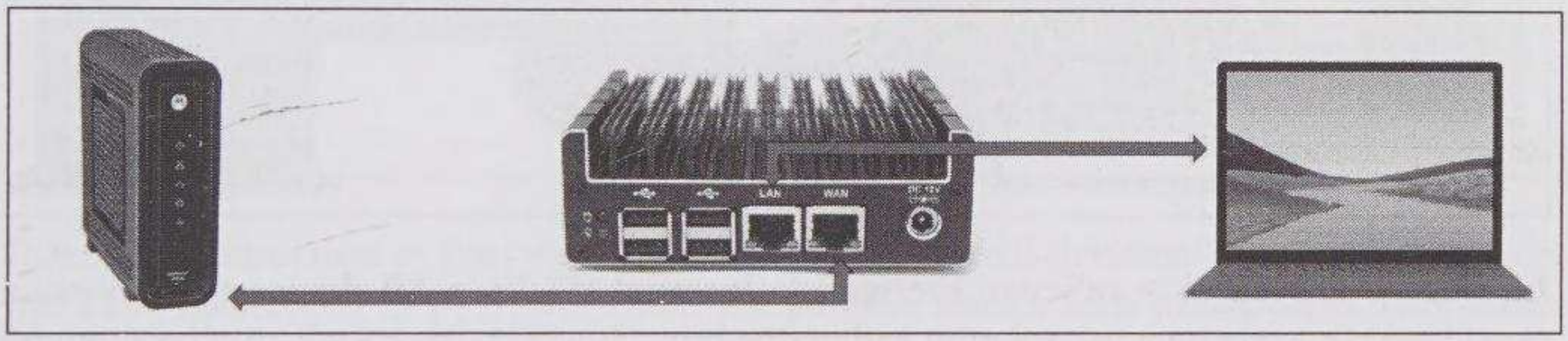
- Within pfSense, navigate to "Interfaces" > "Assignments" > "Wireless".
- Click the "Add" button and make the following modifications:
  Mode: Access Point
  Description: wifi
- Click "Save" and then click "Interface Assignments".
- Click the "Add" button to add the "wifi" device and click "Save".
- Click the new "OPT" option at the bottom and make the following modifications:
  Enable Interface: Selected (checked)
  Description: wifi
  IPv4 Configuration Type: Static IPv4
  IPv4 Address: 192.168.3.1
  /: 24
  Channel: 1
  SSID: pfsense
  WPA: Enable WPA
  WPA Pre-shared key: desired Wi-Fi password
- "Save", "Apply Changes", then navigate to "Firewall" > "NAT" > "Outbound".
- Click the first "Add" button and make the following modifications:
  Interface: OVPNC
  Address Family: IPv4
  Source: Network: 192.168.3.0
- Click "Save", "Apply Changes", then navigate to "Services" > "DHCP Server".
- Click "wifi" and make the following modifications:
  Enable DHCP: Selected (checked)
  Range: "From: 192.168.3.100 To: 192.168.3.150"
- Click "Save" and navigate to "Firewall" > "Rules" > "wifi".
- Click the first "Add" button and change the "Protocol" to "any".
- Click "Display Advanced" and choose a Gateway of "OVPNC".
- Click "Save", "Apply Changes", and reboot the firewall.

During my tests of this configuration, my internet speeds were capped at under 10Mbps. When connected through the Slate wireless router, my speed was 100Mbps. If you possess a slow internet connection and want a simple solution, this may work for you. I do not rely on this strategy due to the low speeds, and I have no clients with this setup.

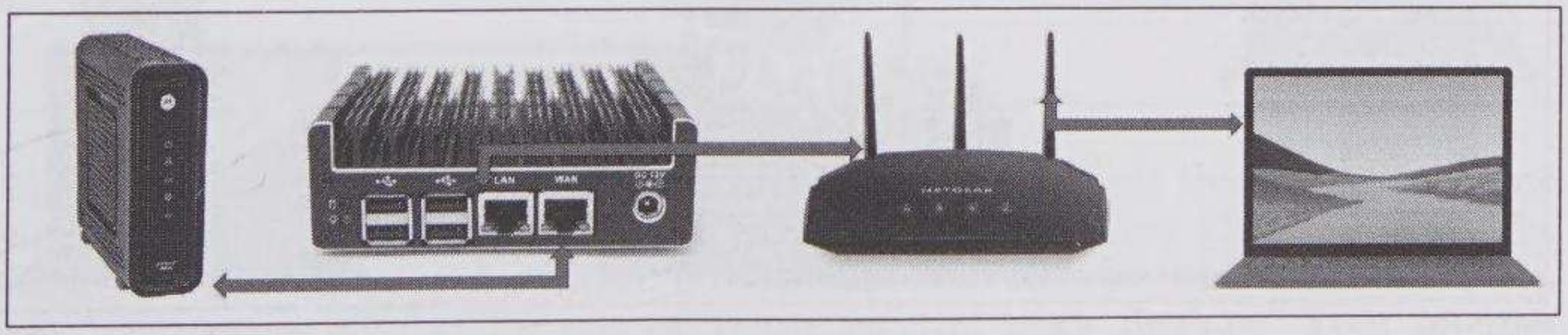
Firewall Summary

This is a heavy chapter. Let's break it down into six categories, starting with the most private and secure, ending with the least private and secure. I present diagrams in order to help explain the concepts after each summary. The modem on the left of each image represents the incoming internet connection provided by your ISP.

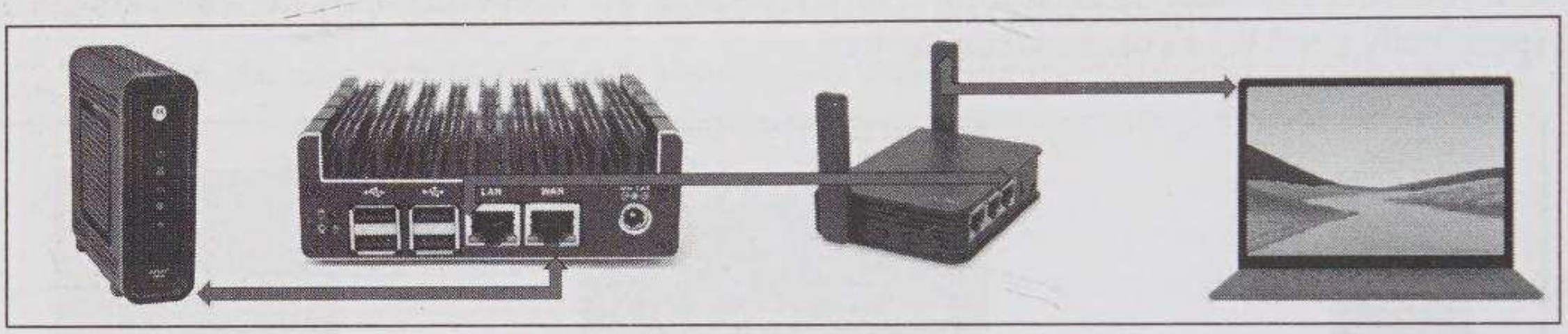
Internet Connection > pfSense Firewall > Wired Devices: This solution provides no Wi-Fi, and should only be considered by those with extreme privacy needs. Your firewall protects all of your internet traffic and you can only connect devices via ethernet wired connections. You will need at least two ports present on your firewall (one for incoming internet and one for your device, such as a laptop). This represents my home most of the time, unless I specifically need Wi-Fi on a mobile device.



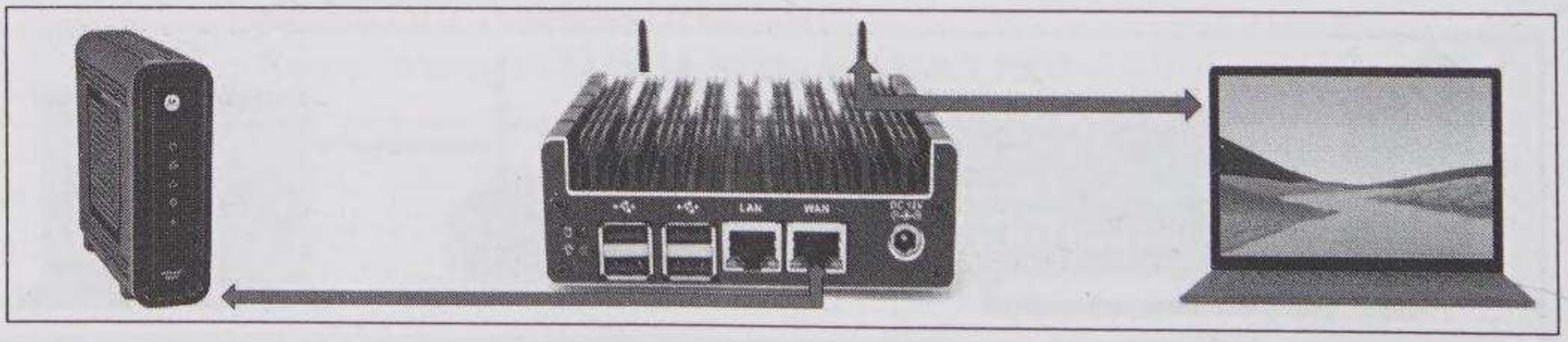
Internet Connection > pfSense Firewall > Open-source wireless router > All devices: This is more realistic for those with other people in the household, and this is the most common execution of this chapter for my clients. The firewall protects all of the traffic in the home with a constant VPN. The open-source wireless router has no proprietary software and all devices connect directly through it. It has a strong range and can support numerous devices. You will be responsible for identifying the appropriate tutorials for installing open-source software such as OpenWRT or DD-WRT in order to replace the stock manufacturer's invasive configuration.



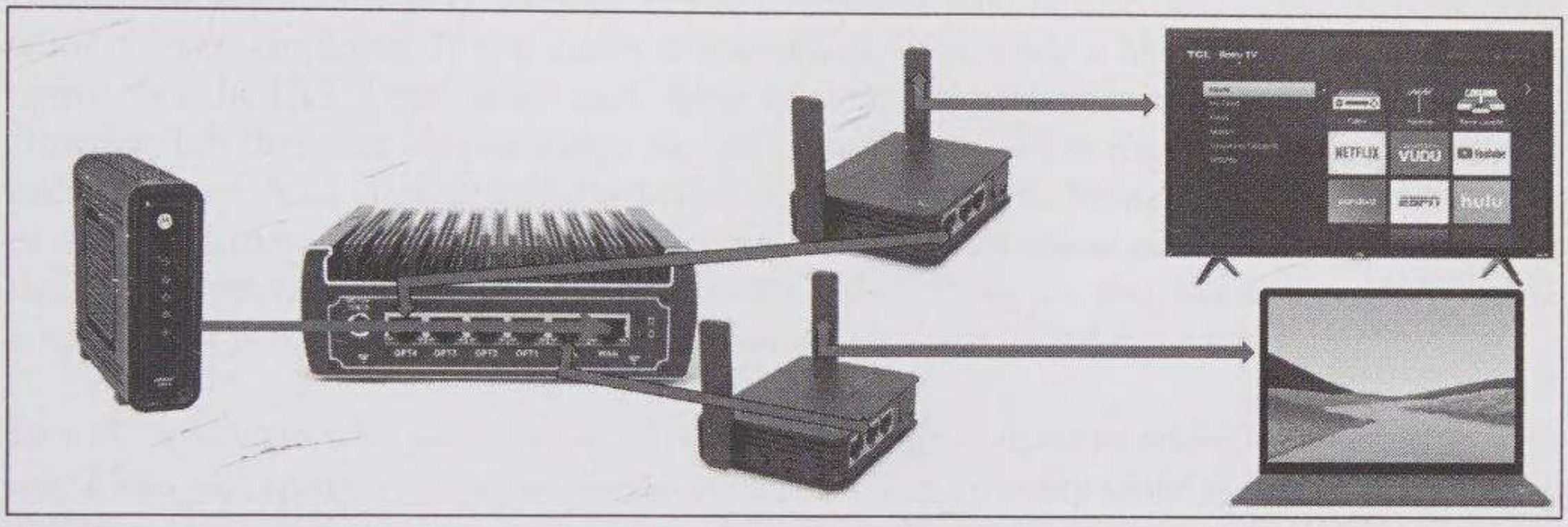
Internet Connection > pfSense Firewall > Portable wireless router > All devices: This is very similar to the previous option, but removes some of the headaches of configuring and maintaining an open-source router. It is the most common scenario for my clients who need a firewall with a static VPN and Wi-Fi which needs minimal configuration. Routers such as the Slate previously mentioned are easier to configure and update. They are ready to use right out of the box. Remember that these devices have a shorter range than traditional home Wi-Fi routers and are not suitable for extremely large homes. However, I have installed these within three-story homes without much issue. One benefit of a less-powerful wireless router is that it cannot broadcast signal too far outside the home. Recently, I installed a Slate within a client's home. I could not see the network from the road, but I received a strong signal everywhere within the interior of the home. This is likely an unintended feature.



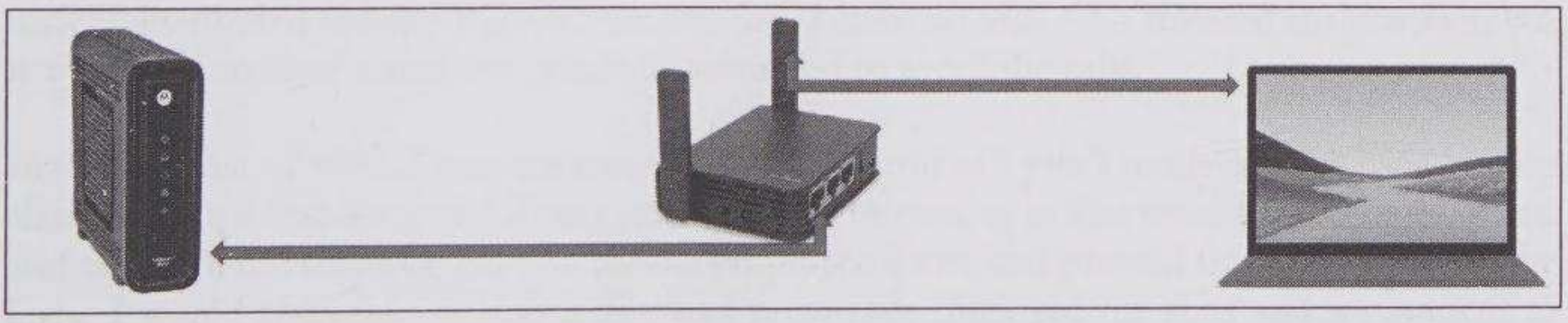
Internet Connection > pfSense Firewall > Internal Wi-Fi > All devices: This option provides a complete network solution within one box. However, the speeds may be slow. All of the Wi-Fi connections are routed through pfSense without the need for an external Wi-Fi access point. I only recommend this for slower internet connections which only require a handful of connected devices. I have also found the range to be less than that of a traditional access point. If your home has a high-speed internet connection which is shared with multiple devices, this is not for you. If you heavily stream high-definition video from various online providers, you and your family will not be happy with this setup. However, this configuration could be used as a standalone travel router. It would provide a stable (yet slow) pfSense firewall with wireless static VPN protection while extending your stay at a hotel.



Internet Connection > pfSense Firewall > "Netflix" port > Wi-Fi > All devices: This option typically results in two Wi-Fi access points which requires two routers. One broadcasts through a VPN-protected network while the other uses a true IP address from a specific port on the firewall in order to facilitate online streaming services. This will be required if you demand privacy and security for your daily internet usage, but your family insists on streaming video services. Pick your battles wisely.



Internet Connection > Portable Router with VPN > All devices: This option relies on the VPN connection as provided within the portable router, such as the Slate. This is not nearly as secure or stable as a pfSense firewall, but would provide your entire home the benefits of a network VPN. Ultimately, this should only be chosen due to financial constraints or temporary needs. This is the most common scenario I present while transitioning clients to extended-stay lodging. You may notice your high-speed internet connection slow down when multiple devices attempt to connect simultaneously.



Finally, a departing note. I firmly believe that every "private" home should have a pfSense firewall in between the internet connection and any devices including a wireless router. The choice of wireless access point (router) is not as important when you have a firewall in place, but I encourage open-source options versus standard stock firmware. **Your internet connection may be the most vulnerable and revealing service you ever use. Protect it at all costs.** As a final reminder, all pfSense configuration scripts can be downloaded from my website at **https://inteltechniques.com/firewall**.

Chapter Eleven

Private Employment

Private employment is easy, as long as you are always paid in cash and never provide your name to your employer. If you are in this situation, your work is likely illegal, at least in the opinion of the IRS. There is no such thing as complete privacy in terms of employment in America, but there are several things we can do to minimize our exposure. This chapter will present many ideas, starting with the least private to the most. None of this is to avoid taxes or skirt financial institution reporting requirements. All of these tactics are legal, and only designed to provide privacy protection from the public. First, you should ask yourself if private employment is important to your overall privacy strategy. Consider the following.

In 1997, a woman who was a friend of mine from 5th grade tried to rekindle a friendship with me. I had not spoken to her in several years, and was not very close to her when we were children. Her initial attempt to contact me was through social engineering. She telephoned my grandfather (listed in the phonebook) late at night and insisted there was an emergency. She asked for my number (a landline), which was unpublished. My grandfather provided my number to my apartment and she began calling me daily. Her voicemails featured incoherent giggling and rambling, and it was obvious there was some mental instability. I ignored the calls.

Within a week, I started to receive voicemail messages from her on my pager (yes, I'm old). My grandfather did not have that number, as it was issued by the local police department where I was employed. I knew that the number was displayed on a call-out sheet which was widely distributed around the city. To this day, I have no idea who released the number, but it was likely another telephone attack. I continued to avoid the calls.

In the summer of 1997, I was working a patrol shift around 9 pm. I received a call for a holdup alarm at a local fast-food restaurant, which would be closing at that time. I raced to the scene and encountered this woman. She was an employee there, and pressed the alarm because she knew I would respond. My dispatcher had previously disclosed my shift and assignment to her over the telephone, after she identified herself as my sister. I called for another unit and she was charged with activating a false alarm. The arresting officer was a close friend of mine who had a heartfelt conversation with her about talking with a professional to seek help. She was later hospitalized with extreme schizophrenia. I do not know where she is today. My point with this story is that your fellow employees will fall for social engineering attacks. While trying to be helpful, they will disclose your home address, telephone number, work hours, and vacation times to anyone who has the talent to present a pretext or ruse. Anything you share with your employer is fair game, so let's choose how we provide sensitive details.

Traditional Employment

Let's start with traditional employment. When you apply for practically any job in America, you will be asked for your name, address, DOB, and SSN. Lately, some companies do not ask for an SSN until an offer of employment is made to you. My recommendation is to never provide an SSN unless an offer is made. If required on an application, I would enter "upon employment offer". This lets the potential employer know that you are willing to cooperate with tax reporting requirements, but do not want to provide your SSN when unnecessary. This prevents accidental exposure of your SSN when these applications are lost, leaked, or sold. They may require your SSN for a background screening, which is acceptable prior to employment if you feel the job offer will soon follow.

If you receive an offer of employment, you will be required to provide these details. This is likely for two reasons. First, most companies do a minimal background check through third-party services such as The Work Number, yet another Equifax product. Your potential employer will disclose all of the details you provided on the application, including your home address, to these services. Any information that a company did not already have about you, such as your new apartment address, will be added to your consumer profile and shared. This is a very common way in which these data mining companies keep such accurate records on us. I would display concerning portions of Equifax's privacy policy here, but it does not matter. The 2017 breach of over 150 million people's full Equifax profiles eliminates any protections cited in their privacy policies. The data is now in the wild.

Second, your name, address, DOB, and SSN are required for legal payment, and will be included on an IRS form W-9. This allows the IRS to monitor your wages and ensure that you are reporting the proper taxes. I would have previously said that this data is private from public view, but the widely reported IRS breach in 2016 assures us this is not the case. Today, I can visit a handful of shady websites and query names from this breach. The free report displays full address history, and a small fee will provide me your DOB and SSN. There is no way to erase this damage.

This is a grim view to begin a chapter about employment privacy. However, I believe we have options to safeguard our information the best we can. First, I would never provide my home address on any application or W-9 form. This should only be your PO Box or UPS Box address. Your employer likely does not care much about where you live, unless the job has residency requirements, such as a police officer. The IRS does not object to the use of a mail box address. They just want their money. The majority of potential employers never require to know where you truly reside.

Next, I would have a credit freeze in place before submitting any application or tax form. This will be discussed later, but it basically locks down your credit from unauthorized queries.

Companies such as Equifax can bypass this since they own the data. However, smaller companies that are hired to conduct background checks will not always be able to peer into your credit if you have a freeze in place. If you expect you will be releasing your SSN to unknown third parties during your job hunt and eventual employment, you must assume it will be handled carelessly. The credit freeze gives you major protections if and when a malicious actor stumbles across your DOB and SSN.

Once you are hired, there are likely to be more invasive requests. Many companies maintain a contact list of all employees which includes names, home addresses, personal telephone numbers, birthdays, and other unnecessary information. Expect these to be compromised and become public information. If pushed for a personal cell number, provide a MySudo or other VOIP number. If asked for a home address, insist on only displaying the PO Box or UPS Box previously provided. If questioned about this, claim you are moving very soon and will provide the new address once you have everything moved in. Conveniently forget to update this.

There are many careers where this does not work. Police officers, fire fighters, elected officials, and other government employees must disclose their true home addresses. This is usually to satisfy residency requirements set forth in outdated municipal laws. My first suggestion is to obey the residency requirement. If you must live within 20 miles of the police department where you work, meet this demand. Then explain your privacy concern to the proper personnel and request that your true address is not documented on any internal forms. This is a difficult task, and you may be met with great resistance. I know many people that have "shared" a low-cost vacant apartment in order to provide that address to their departments. I cannot recommend this. I can only say it has been done. If you are a public official, you have likely already given up much of your right to privacy.

Employee Identification Requirements

My first "real" job was at a local hospital. All employees were forced to wear employee credentials which included full name and a photograph. During my first day, a human resources representative captured my photo with a Polaroid camera, physically cut the photo to the appropriate size, and laminated it within my "name badge" while I witnessed the entire process. Things were much simpler back then, and I saw no privacy invasion with this mandate. Today, things are much different. Many companies capture a digital photo with a dedicated employee identification system. The digital image is either stored internally at the company or shared to a third-party credential maintenance system. In either situation, leakage is possible. My bigger concern is the abuses which I have witnessed, such as the following.

- A technology-related company created Gravatar accounts for every employee's email address and uploaded images to each. Every outgoing email now possesses the face of the employees served as an icon in the sender field.

- A telecommunications company uploaded the photos of employees to their website and associated each with full names. Today, several archives are available to the public. These employees can never completely remove these images.
- Another technology company forced all employees to participate in a Slack-style online communications platform. The company attached images of employees to the profiles, which were scraped by various online people search websites. Today, these public search sites display photos of the employees next to home address and telephone details.
- A police department shared the photos of all employees with the local newspaper. Today, whenever a police officer is mentioned in an investigation, the newspaper includes the photo of that person. The Associated Press has replicated many of the articles (and photos) nationwide. These photos are present on hundreds of websites.
- A financial company created caricatures of employees based on the identification photos and placed them online. Most images displayed enhancements of physical features that most would not want highlighted. These cartoon versions humiliated employees by magnifying big noses, acne, thick glasses, and in one unfortunate image a facial scar received after childhood physical abuse. These images were later posted to social networks by "friends" of the employees. The comments attached to the posts were crude and demeaning.

All of these scenarios happened without consent from the employees. This type of exposure may be outside of your threat model. However, I urge you to consider any future vulnerabilities. If you are ever charged with a crime or misdemeanor traffic offense, media outlets will try to find the most unflattering photo available. If a fellow employee becomes upset and seeks revenge against you, these photos can be abused on social networks and other online sites. I recently had a client contact me after her head from her employee identification was Photoshopped into pornography and posted online. We know that people can be cruel and there are endless ways to abuse digital images, but what can we do about it? Employers likely require images of employees, and the systems to store this data usually possess no security. I have no magic solutions, but I do offer a few considerations, in order of most advised to least.

- Have an honest discussion with your employer. Explain that you have specific reasons to protect your privacy, and you respectfully request that your image not be captured and stored by the company. Explain the vulnerabilities mentioned previously and identify how you may be negatively impacted by abuse of the images.
- Request to review any policies which require photographs of employees. Additionally, request details about the storage, sharing, ownership, and online publication of the images. You will likely find out that such policies do not exist. You could ask to

postpone any employee photos until the protection policies are in place. This may generate unwanted attention from your superiors, so approach cautiously.

- If appropriate, explain that you have a religious objection to captured images. Some have referenced the second of the ten commandments, which partially reads "Thou shalt not make unto thee any graven image or any likeness of anything". A few denominations, such as the Amish and Old Order Mennonites, often refuse to have their photographs taken due to this wording. Expect eyerolls if you go this route.

As a new employee, you may not want to become too forceful with your requests. Please consider any consequences before execution. Seasoned employees may have an easier time refusing employee photos as they may possess more job security. I present this section simply to create awareness of the issues surrounding employee photos. Your results may vary.

Company Parking Permits

In 2019, I began witnessing a new privacy invasion from employers. Businesses began demanding full vehicle details of every employee, all of which are commonly stored within a third-party verification system, and of course shared with other companies. In 2020, the make, model, color, VIN, registration, and insurance details were requested from one of my clients. She had conducted a full privacy reboot and did not want her vehicle associated with her true name. When she questioned the necessity of these details, the employer only stated it was a new policy.

When we took a deeper dive into this, we discovered that the details were being provided to a third-party parking management company. The employer had outsourced the parking garage to another business. Big deal, right? Who cares if a third party knows what type of vehicle you drive? Well, you should. The parking company which requested the details of my client's vehicle also associates the following information to the employee's profile.

Date and time of each entry into the garage (When she arrives to work)
Date and time of each exit from the garage (When she leaves work)
Length of stay (The number of hours she worked)
Average length of stay (The average hours she works)
Daily average length of stay (The days she works less than others)
Photograph of each entry (A daily image of her driving the vehicle)
Photograph of each exit (Another daily image of her driving the vehicle)
Optical Character Recognition of the license plate (Searchable log of all usage by her vehicle)

To add insult to injury, the privacy policy of this provider clearly states that they can share or sell any information with any third parties solely at their discretion. This is very invasive toward someone who has gone through the steps in Chapter Six in order to publicly separate their

vehicles from their true identities. Similar to the previous section, there are no fool-proof strategies to prevent the collection of these details. I present the following consideration.

Most of these scenarios include a physical parking permit which grants access to the parking areas. The details of the vehicle are not necessary in order to enter the parking areas, but usually gathered for record keeping. My client informed her employer that she was currently driving a rental vehicle and would disclose her true vehicle information once she received it back from repair. She "forgot" to update the record and continued to park her true vehicle in the garage without any repercussion. However, a few months later, the company again demanded the details of her vehicle. The next day, she arrived to work in a rental vehicle and provided the make, model, color, VIN, and registration. Her employer was content and shared the details with the parking company. She returned the rental and continued using her true vehicle the next day. Her rental vehicle cost was under $30.

She cannot prevent the system from tracking the usage of her parking pass or capturing images of her activity. However, the system does not have any record of her VIN or registration. This protects the identity of the owner of the vehicle, such as a trust or LLC. Her magnetic plates, as explained in Chapter Six, are removed the moment she leaves the public roadway and enters the private property of her employer. This is legal, as there are no vehicle registration requirements on private property. Is this overkill? Probably. However, she enjoys the rebellion, and benefits of privacy.

Mandated Licenses

Many careers require a government license. These include hair stylists, Ham radio operators, nurses, veterinarians, and many other professions. The details of these licenses are public record. If you are skeptical, navigate to www.myfloridalicense.com/wl11.asp and type in any generic name. The results include full license details such as name, home address, telephone number, license acquisition date, expiration, and profession. If you require a specific license for your employment, only provide a PO Box, VOIP telephone number, and burner email address. This information will be abused.

Some careers have more exposure than others. I am consistently contacted by celebrities and politicians seeking more privacy. While I can provide anonymous lodging and alias payment sources, I cannot remove them from the spotlight. There is nothing I can do to make Tom Hanks completely invisible (but I am willing to try if he should call me). You should consider the overall exposure of the type of employment you are seeking. If you have a public presence, you risk exposure in newspapers or the local television news. If you work for a private company inside of a building all day, your risk is minimal.

Most of my clients just want to fade into the background with the most minimal amount of attention possible. Overall, traditional employment will always expose your name, DOB, and SSN. In most scenarios, you can keep your home address and cellular number private. The rule is to always assume that any details provided at any time during the employment process will become public information. If we go in with this attitude, any damaging exposure should be minimal.

Technology in the Workplace

Consider a few more tips in regard to working inside an employer-owned building. Much of this may seem redundant from Chapter Three. Previously, I explained ways to protect yourself digitally while in your own home and within spaces which you have control. When at work, you are much more vulnerable. I believe you are more prone to eavesdropping attacks. The following is a short list of tactics which should be executed while at work.

- Cover webcams on any employer-owned computers or portable devices.
- Insert microphone plugs into employer-owned computers.
- Never use personal devices for work-related tasks.
- Never use employer-owned devices for personal tasks.
- Never use your work email for personal communication.
- Never use your personal email for work communication.
- Never use your work cell phone for personal communication.
- Never use your personal cell phone for work communication.
- Never connect to personal email accounts from employer networks or computers.
- Never connect to work email accounts from personal networks or computers.
- Never connect personal devices to employer-provided Wi-Fi or Bluetooth.
- Never connect employer-provided devices to personal Wi-Fi or Bluetooth.
- Never connect personal devices to USB ports of employer-owned computers.
- Never connect employer-owned devices to USB ports of personal computers.
- Faraday bags should be used for personal devices to block wireless scanning in offices.
- Refrain from sharing details of your employment within social networks (LinkedIn).
- Request your birthday (DOB) be eliminated from celebratory email blasts.

Self-Employment

Contrary to traditional employment, self-employment can provide many advantages in regard to privacy and digital security. If done properly, you will never need to disclose your DOB, SSN, or home address to any entity. You can be paid through an LLC which possesses a valid EIN from the IRS, which is much more private with less risk of public exposure. Your first task would be to identify the type of work you desire.

There are countless career choices for the self-employed, and I am not here to guide you into any specific direction. I have had clients who possessed their own home-based businesses, conducted on-site training and consulting, and ran various online stores. Only you can decide what type of business fits best with your personality and experience. My goal is to guide you through the process of making your choice legal and private.

Your first task is to establish the legal infrastructure for your business. This was previously discussed as a privacy tactic for asset ownership. The process for establishing a business which anticipates income is very similar. The LLC documents previously mentioned can be used for your new venture. However, there are many considerations for the public filing of your new business.

During the previous legal infrastructure chapter, the goal was complete privacy. I discussed the New Mexico LLC which could shield the true owner of an LLC from public view. In my opinion, this level of privacy is not vital for a business which will be used to generate income. You will be required to disclose your true identity to the IRS and any financial institution which you use for payments and distributions. If you will be conducting any type of consultation, training, or other services, your name is likely to be associated with the business in some form. Therefore, I don't strive to hide the identity of the owner of a business.

The first step is to establish your LLC in the state which you reside. For a small number of readers, that may by the state where you established nomad domicile, such as South Dakota. For most of you, it will be the state where you own a home or possess a driver's license. Every state has their own rules, and you should spend some time reviewing the state's business entities website. There are also many local businesses which will assist you with establishing the LLC (at a substantial cost). If you have made it this far into the book, I have no doubt that you can do this yourself.

At a minimum, the state will want your name, address, email address, and telephone number. The address you provide can be a PO Box or UPS Box, the email can be a ProtonMail account designed specifically for business use, and the telephone number can be any VOIP service you use. As with the previous lessons, everything you provide will become public record.

Nomad Business Registration

In order to possess extreme privacy, you might consider the nomad residency route discussed earlier. If you do, you have the ability to legally establish a publicly invisible LLC which can be used to generate income. The IRS will know you are connected, but this method provides many privacy strategies unavailable to traditional employment. The following scenario assumes you are a legal nomad resident of South Dakota and you possess a PMB and government identification from that state.

The first task is to choose the name of your new LLC. This needs to be something that is not already in use in the state. I prefer generic names which could describe anything such as Ventures Unlimited LLC or Consulting Group LLC. Conduct a search at the following website. While you are there, take a look at a typical completed application, which is visible on the business details page.

https://sosenterprise.sd.gov/BusinessServices/Business/FilingSearch.aspx

Next, you should decide which address you will use for the LLC. While you could use the South Dakota address provided by Escapees, you may choose another option. For extreme privacy, I prefer to use a unique address for my business. This creates another layer of privacy and does not expose my "home" address publicly. This also provides an opportunity to choose a PMB provider which can also act as your resident agent. Similar to the New Mexico example in a previous chapter, a South Dakota LLC requires you to possess a registered agent within the state. For most clients, I use Americas Mailbox as the business PMB.

I am reluctant to promote Americas Mailbox. I have had several problems with their service over the years. Missing mail has been an issue and their customer support staff are rarely helpful. On one occasion, they marked the wrong box on a vehicle registration and entered a lien for a car paid with cash. It took several months to get that straightened out, and Americas Mailbox insisted they did nothing wrong, refusing to apologize or pay the fees. On another occasion, I received a mailing from the state five months after it arrived. However, their new scanning feature allows me to cautiously approach their service again.

The procedure for establishing a PMB at Americas Mailbox is the same as previously mentioned with Escapees. You can find the application process online on their website at http://www.americas-mailbox.com/Forms/Full.App.Kit.pdf. Be sure to select the scanning feature and the registered agent service. This will add a minimal fee to your annual plan, but will keep you legal with the state. Contact the service and ask which name you should provide as your registered agent. You will need that for the state application process. Your new PMB address should only be used in connection with your new business. You will be required to submit a USPS form confirming your identity as you did with Escapees. You can use your

Escapees address on this form. Be sure to list your LLC name as a confirmed recipient on this form. I also include my Contract Officer's name, as explained momentarily.

Once you have confirmed your PMB with registered agent service, the next task is to apply for an LLC with the state. This is done online, and the result is immediate. In previous years, applications required physically mailing the documents and waiting for a confirmation. The entire process now takes less than ten minutes. This is extremely beneficial. Some states, such as Washington, require months of verifications and other processing before an LLC is approved. Navigate to the following website.

https://sosenterprise.sd.gov/BusinessServices/Business/RegistrationInstr.aspx

The site will walk you through the process, prompting you to make decisions along the way. Avoid completing any "optional" fields. The application process is split into twelve categories. The following provides notes on each.

- **Business Name**: The name you selected after confirming it has not been taken.
- **Addresses**: Any address information should be your new PMB.
- **Agent**: Select the "Non-Commercial" option and enter the name of your agent provided by your PMB. Conduct a search and choose the appropriate option.
- **Organizer(s)**: You can select an individual or a company for this. South Dakota allows you to specify your own LLC as the organizer, which I find interesting. If you would rather assign an individual, you can add your own name or another "nominee". I have a close friend with a very generic name such as John Wilson. I pay him a small annual fee to be my "Contract Officer", and he has the authority to "Organize" my business. His address is not required.
- **Detail**: Choose "Perpetual" in order to set no specific expiration date.
- **Manager(s)**: Select the "Member-Managed" option and "No".
- **Beneficial Owner(s)**: Optional field to be avoided.
- **Additional Articles**: Optional field to be avoided.
- **Recipient**: Optional field to be avoided.
- **Confirmation**: Make sure everything looks right.
- **Signature**: This is a digital input and no "wet" signature is required. The name you provide will be public record. I ask my Contract Officer to be the authorized signee on my LLCs.
- **Payment**: You can pay with a credit card, prepaid card, or Privacy.com card, depending on your desired level of privacy.

After successful payment, you will immediately receive a digital copy of your Articles of Organization and Certificate of Organization. You now possess an official and legal LLC in the state of South Dakota. If you are not a nomad in that state, you should consider creating an LLC within the state of your residence (or domicile). The steps should be similar, but each state possesses its own nuances. Some states can be very invasive and demand to know the full details of LLC ownership. If using the LLC for income, this is not a huge concern, as the business will be associated with you anyhow. My only mandate would be to never disclose your true physical address within any registration documents. It will become online public information within days.

IRS Registration (EIN)

If you plan to ever generate income in the name of the LLC, or open a business checking account, you will need an EIN from the IRS. You can bypass this if you plan to funnel income directly through your own SSN, but that defeats the point of the business as the wall between your identity and your income. Obtaining an EIN is simple and immediate at the official IRS website located online at https://sa.www4.irs.gov/modiein/individual/index.jsp. You can complete the application any time from Monday through Friday, 7 a.m. to 10 p.m. Eastern Time. The process will demand your full name, address (PMB), and SSN. There is no legal way to facilitate an EIN without making this connection. Fortunately, this data will not be (intentionally) released to the public.

I believe an EIN is vital for private employment. It allows me to truly segregate my personal information from the various public disclosures that are associated with accepting payment. Every time a client/customer requires a tax form, I can keep my SSN private. If I need to complete registration through a third-party vendor, my name can stay out of it. Most importantly, I can now create a business checking account for deposits and payments. This new account can continue the public isolation from my true identity.

It is important to note that an official LLC is not required in order to obtain an EIN from the IRS. A sole proprietor (individual) can obtain an EIN at no cost without any official state business documentation. This does not provide all of the protections of an LLC, but can allow you to isolate your SSN from clients requiring a tax form. I generally do not recommend sole proprietor EINs because they still require you to disclose a full name to customers and provide no liability protection. However, some may find them to be beneficial. The EIN issued to a sole proprietor will be similar to that assigned to an LLC. There will be no distinguishable features which would identify the type of registration.

Bank Account

Banks in America must follow strict government regulation in terms of opening new accounts. Know your customer, alternatively known as know your client or simply KYC, is the process of a business verifying the identity of its clients and assessing potential risks of illegal intentions for the business relationship. If you wish to open a new bank account in your business name, you simply must disclose your true identity and association. Consistent with previous instruction, I always recommend seeking locally-owned banks and credit unions instead of large chains. They will have less requirements and offer better privacy. When you open a new account, you will need the following.

Government identification
LLC Articles of Organization
LLC Certificate of Organization
IRS EIN confirmation

In rare scenarios, they may wish to view your LLC Operating Agreement. I have allowed this, but I do not allow a copy to be made. This agreement contains sensitive details such as your shares of the company and specific organization of members (if applicable). As long as you are forthright with your true name and proof of PMB address, you should have no issues opening a new account. You will be asked for a deposit into the account, which then allows you to use typical checking features. As before, I always request as many "temporary" checks as the institution will allow upon creating the account. I also request that a mailing address is absent and that only the business name appears on them.

Credit Card Processing

In my experience, many potential clients or customers will want to pay you with credit cards. This can be very simple with popular privacy abusers such as PayPal, but I never recommend them. PayPal currently shares your data with over 600 third-party companies, and appears amateur on an invoice. Instead, consider better options. I recommend Stripe or Square for all credit card processing. They are not perfect solutions, but they possess much cleaner privacy policies than PayPal or other payment collection options.

Stripe will require your full name, SSN, DOB, business name, and LLC EIN. This is required per the KYC demands as previously mentioned. Once you are approved, you can insist on the EIN receiving the tax forms (if required). The true power of Stripe is the ability to embed its software into your website, but that is probably overkill for most small business owners. Most of my clients who own small businesses simply send electronic invoices straight from the Stripe dashboard on their website. The recipient can pay via any credit card, and you receive

the funds within a couple of days. Stripe will want to know where the funds should be deposited, and I recommend the business checking account previously mentioned.

Square is almost identical in regard to account creation requirements. The additional benefit of Square is that they will issue you a credit card reader, which allows you to physically accept credit cards through any mobile device. Both options will charge you a fee of approximately 3% of each transaction.

Virtual Currency

As previously stated, cryptocurrencies such as Bitcoin can provide a great layer of anonymity. If you provide a service of interest to those in the virtual currency world, you should be prepared to accept Bitcoin. Use the techniques discussed in Chapter Nine to create and configure your own Bitcoin wallet. Advertise that you accept Bitcoin, either through a website or in the physical world. Consider my adoption of Bitcoin.

From 2013 through 2020, I offered online training courses. 99% of the purchases were made with a credit card on my site through Stripe. However, I also advertised that I accepted Bitcoin. Over those years, I slowly built a wallet full of Bitcoin without the need to create an account through an exchange. I now have funding in this wallet to pay for various online services. I still needed the credit card transactions in order to keep my business afloat, but the incoming Bitcoin provided a strategy to obtain it anonymously.

Contractor Considerations

When you begin conducting business with larger organizations, you will find many of them have their own vendor registration requirements. These can be a deal-breaker for me. Some are minimal and only require the information that you have already made public via the steps previously mentioned. However, some are extremely invasive, and I will present a few scenarios here.

Overall, government vendor portals are the worst privacy offenders. In 2012, I was hired to teach a course for a military organization. They required me to be registered in the General Services Administration System for Award Management (GSA SAM) website at SAM.gov in order to receive payment. I was naive and assumed that my data would be protected. I provided my full name, actual physical address, and my personal email account. This became public data and was immediately shared with hundreds of other businesses. I began receiving unsolicited offers to help grow my business and learn how to navigate federal contracts (for a fee, of course). Today, I still receive email from these outfits, even after I completely removed my registration.

Many companies will require you to be registered in the Dun & Bradstreet (D&B) database in order to collect payment for services. This private organization has somehow become the minimum standard requirement for private and government contracts. At least once a month, we must turn down a potential client because they demand we share our data with D&B. While their privacy policy is riddled with concern, a single paragraph sums it up:

"Dun & Bradstreet shares information with third-party service providers, such as credit card processors, auditors, attorneys, consultants, live help/chat providers and contractors, in order to support Dun & Bradstreet's Internet websites and business operations…We may also disclose the information as required or appropriate in order to protect our website, business operations or legal rights, or in connection with a sale or merger involving Dun & Bradstreet assets or businesses…From time to time, Dun & Bradstreet compiles online and offline transaction and registration information for internal analyses, such as market research, quality assurance, customer experience, and operational benchmarking initiatives."

In other words, they can share your details with anyone. Even worse, D&B has already had one known breach that exposed the profiles of over 33 million businesses and owners. Why should this matter when the business details are already public? The reason is that D&B requires much more invasive information in order to have the privilege of them selling your data. This includes the following:

Full name of owner (not just the business name)
Physical address of owner (no PO or PMB allowed)
Telephone number (no VOIP allowed)
Employee details

I applied for, and received, a DUNS number from D&B in 2013. During a regular reminder in 2016 to verify my company information, I was prompted to enter a valid physical address. I had my PMB on file, which was now being rejected. I attempted to enter a handful of business addresses, all of which were denied. Without my true home address, I could no longer possess a valid registration. I happily deleted my profile, and I have not had one since.

Local municipalities are also reckless with your information. In 2015, I was contracted by the city of Reno to conduct an OSINT training course. The course was canceled after they could not locate a venue, but the contract was published to their website. It displayed my name, PMB, full details of the event, and my signature. I had to make several requests to redact my address and signature. After much hesitation, they finally modified the online document. Again, you must assume that every detail provided to a client will be made public.

The purpose of a private business entity is to shield you from personal data exposure. If you have created your own LLC properly, you are prepared to conduct legal business and accept

payment while never disclosing personal information. Consider the following typical invasive procedures, each of which include the public information which you can provide without risk.

W-9 Form: As a sole member LLC, or partnership LLC, companies are required to submit proper tax reporting to the IRS if you are paid more than $600 yearly. Legitimate companies will require you to submit an IRS W-9 form. You only need to disclose your business name, EIN from the IRS, PMB address, and an illegible signature. The IRS can later verify your actual income with your reported earnings. Your name does not need to appear on the W-9.

Vendor Paperwork: If you conduct work for large organizations, they will demand you be entered into their third-party vendor systems. These are notorious for leaking details into public records. You can provide only the business name, PMB address, business ProtonMail email account, burner telephone number, and IRS EIN. If they insist on a contact name and signature, you can appoint anyone as a nominee for this. My good friend with the extremely generic name mentioned earlier is paid a very small annual fee to be the official contact and signature on many contracts. He is my "Contracting Officer".

Payment Records: Many government entities are required to publicly disclose all payments to third parties. You may see these notices on local newspapers or on websites. This data is collected and aggregated by various data mining companies. When this happens, I prefer my LLC to be listed instead of my name. Your LLC prevents personal exposure.

The weakest link here is the IRS. They can connect you to your LLC through the EIN. I do not see this as a threat for most people. I would much rather provide my EIN to strangers than my SSN. Hiding my SSN protects me from rampant tax return fraud. Supplying a business name instead of my real name to business clients prevents an easy lookup on various people search sites. When the details of my business become public, my name is not present on the vendor forms.

If you possess a nomad residency and South Dakota LLC, you can safely share business details and remain private. The address provided within the various documents required by your customers is not a risk. It displays a physical address you have never visited. That PMB service does not know where you live. The EIN provided cannot be abused as much as an SSN. A DOB should never be required, and the creation date of the LLC can be provided when demanded. You possess a great shield that protects your personal information.

This may all seem invasive for a book about extreme privacy. Remember, this LLC is only required if you plan to generate income under a business name and do not want to publicly disclose your personal details. In order to better explain how all of these steps can help us achieve better privacy and security, please consider the following true scenarios from my own LLC use.

- I was asked to submit a W-9 in order to be paid for an on-site consultation. My W-9 displays my business name, business PMB, and EIN. My name and SSN do not appear. This is now kept on file at an accounting desk which likely possesses minimal security. If it leaks, I really do not mind. The PMB address is not my personal PMB address, and I have never physically been inside either.
- A government entity publicly posted all payment on their website. My business name and the amount I was paid is present. Searching my name will never reveal this information. Searching the name of the LLC reveals my organizer, but not me.
- A company required me to comply with their vendor registration demands. The data provided was shared with an employment verification service and added to their own database. Neither system possesses my name, SSN, DOB, or personal address. The data being shared and re-sold does not compromise me personally.
- I needed to make a payment from my business checking account. I do not possess a credit card in the LLC name. I created a Privacy.com account and associated it with my business checking. I now use debit card numbers to make purchases without risk.
- I presented a keynote at a large conference. My speaking agency only supplied my business details and contact information during my registration. A complete roster of all attendees and presenters was given away, including names, home addresses, telephone numbers, and email addresses. My entry contained no sensitive details.
- I provided training at a BlackHat event in Las Vegas. Only my business details were given for payment, which were eventually shared with all of the vendors at the event. My name was not present on any of the promotional instructor details. The address provided is a mail drop with no public association to me.
- The state knows the business name, but not my name. The address on file is a PMB with no public association to me. Searching my name with the state reveals no records. Searching my business name does not reveal my name or personal PMB address.
- The IRS knows my true name and that I own the business. The addresses on file are both PMBs. This data is not (intentionally) public. Identity theft criminals usually focus on personal tax profiles instead of business filings.
- My bank and credit card processors know my true name and that I own the business. It does not know a true physical address for me nor my personal PMB address. A search warrant would be required to disclose the relationship.

I openly provide my accountant with all income, expenses, and tax documents. I legally comply with all state and federal tax reporting requirements. The IRS takes their share and is happy. The state in which I physically reside gets its cut when I file my state tax return, using a local PO Box as my physical address. Whether you choose traditional employment or decide to become self-employed, there are many privacy strategies ready for you. You must be diligent whenever personal details are requested. Always expect that any information provided will become publicly available.

Chapter Twelve

Anonymous Pets

My dog has two aliases. Please continue reading and let me explain before you dismiss this chapter as pure paranoia. My German Shepherd is named Riley. His aliases include Kosmo and Lightning. Surprisingly, obtaining and maintaining a pet anonymously takes a lot of effort. Paying cash to a home-based puppy breeder is easy, but every pet related encounter past the original purchase is extremely invasive. The shelters offering rescued pets are funded by pet marketing companies, veterinarians, and pet supply organizations. Many counties share vaccination records with third parties. In all of these scenarios, your personal information as a pet owner is valuable, and abused.

In 2018, I had a client who completed my entire program and possessed a completely invisible home. She had no connection from her real name to her home or the area where she lived. She was running from an extremely abusive person, and her ability to live safely required her to stay off radar completely. After settling in, she wanted to adopt a dog from the local shelter. Since the shelter was constantly pushing dogs and always overcrowded, she assumed this would be an easy task to complete anonymously. She showed up, looked around, and fell in love with a young mixed-breed dog. She played a bit, went for a walk, and was determined to take the dog home that day. She approached an employee at the shelter and shared her intent. The employee handed her an application for adoption, and it all went downhill quickly.

Obviously, the application wanted a full name, address, telephone number, and all other basic details. My client was a pro with this, and had an alias name ready to go. However, she was immediately stopped in her tracks. The shelter demanded to view, photocopy and maintain the copy of her state issued identification. Furthermore, they reserved the right to visit the home for an inspection. The final nail in the coffin was demanding the right to share all submitted details with third parties including pet insurance companies, lost pet services, and social networks. She was a bit devastated. She left alone without a companion, and contacted me requesting assistance. The following details may be received with anger or skepticism. As an animal owner and advocate for adoption from shelters, I stand by my actions. As long as the animal is given a loving home, I have no objection to bending the rules a bit in order to maintain privacy. You will learn how standard pet adoption with your real information populates public databases within months and exposes your details for the world to collect.

My client lived in a popular urban area, and I had a meeting with another person in that area when this client reached out about this problem. I was able to meet this client at the shelter in order to get a feel for the operation. It was similar to every other animal shelter I had seen,

and was very similar to the shelter from which I obtained Riley. It possessed overworked and caring staff with strict rules in order to prevent animals from going to abusive homes. I obtained an adoption application and confirmed everything my client had told me. The shelter was on top of their game.

I walked around, played the role of a potential customer, and made small talk with a handful of employees. I executed the best social engineering attempts of my capability, and struck out non-stop. I failed with each of these pretexts.

"I really value my privacy, and I simply do not want to provide a copy of my license. I am open to a home visit, but I have been the victim of identity theft several times and refuse to add to that mess."

"I am a full time Canadian citizen, so I only have a passport. It is illegal to copy a Canadian passport. Can I offer anything else?"

"I don't drive, and have not had a state ID for many years. What else can I show you? A Utility bill or cell phone statement?"

There was no budging. If I could not provide government identification and proof of residency, they would not release an animal to me. If I refused to sign the waiver to share data with third parties, I could not adopt a pet. This is actually very common, and I was not surprised. My client and I left the shelter and began discussing our strategy.

At first, my client was open to just releasing her real name and address, and trusting that it would not be made public. After all, who would an animal shelter give the data to that would have any real impact? You might be surprised. This shelter released the entire application to the following organizations, which then used the data as explained.

24PetWatch: This service provides a free portal for shelters to use for microchip identification. When the shelter gives you the animal, they update the microchip pet record with services such as 24PetWatch. For the shelter, this is a great deal. They get free microchips, readers, and the ability to update records nationally. However, 24PetWatch gets even more benefit. They get your personal details and the pet information. This is then used for marketing, as 24PetWatch offers many premium services such as pet insurance. Should you care that services like these have your name and home address? Let's take a look at excerpts from their privacy policy:

- "By registering as a user with 24PetWatch you consent to Pethealth Inc., its subsidiaries, affiliates, trademarks, brands, and partners contacting you and collecting,

using and disclosing your personal information for its own use and/or to any of our service providers."

- "We may need to disclose the personal information we collect to affiliates, subsidiaries, partners, successors and other service providers or agents who perform various functions for us."
- "We may also use this personal information to assess your future needs and to offer the products and services selected by us that may best meet those needs, from affiliates, reputable organizations with which we have strategic alliances or ourselves."

In other words, they can share, trade, or sell your details to any company or outfit they choose. This can then make its way to data breaches and marketing databases. Eventually, you can expect to see your details within data mining companies and people search websites.

Local Veterinarians: Most shelters have relationships with local veterinarians. These relationships help the shelters obtain services such as spaying and neutering at a severely discounted rate, if not free. In return, shelters often share all of the adoption details with the vets in order for the vets to obtain new customers. The result is often unsolicited mail to the name and address on file and occasional sharing of this data with third-party affiliates. In this case, one vet automatically enrolls you with their patient portal VetScene.

VetScene: This is a portal often used by veterinarians in order to have better communications with their patients. Ultimately, it is a way to bombard you with mailed offers of premium services and reminders of upcoming appointments. The fees to VetScene from the veterinarian are often justified due to the influx of new money spent on services and otherwise avoided vaccines and appointments. Their privacy policy contained the usual suspects, such as implied consent to share all details with third parties.

I hope that you are now convinced that providing your personal information to an animal shelter will definitely expose you to numerous third-party data companies. This may be acceptable to you, and I hold no judgement. Since you have made it this far in the book, I must assume that you do not want to consent to this exposure. In order to protect the identity and location of my client, we executed the following strategy.

The first step was to volunteer. When I requested the adoption application, I also requested a volunteer application. Since most shelters are desperate for volunteers, they do not always scrutinize these applications. While the shelter definitely wanted the same details as for an adoption, they did not demand identification to volunteer. My client completed the volunteer application with her alias name and real address, and provided a VOIP burner telephone number as a contact option. She gave the completed application to the shelter and scheduled her volunteer training session for the following week.

She began volunteering twice weekly at the shelter. She walked dogs, helped at public events, and most importantly made friends with the staff. The relationships she started to foster turned her from a potential customer to a friendly volunteer who could be trusted. The dog that she wanted had already been adopted, but this gave her an opportunity to learn more about the shelter, their privacy policies, and be around numerous potential lifelong pets.

Three weeks into her volunteer journey, the original dog that she wanted was returned to the shelter. The family that adopted it could not tolerate the energy and was not able to provide the patience and discipline required to raise a happy dog. My client contacted me right away and said she wanted to jump on the opportunity. She admitted that she did not possess any friendships that would waive the adoption requirements, but that she was a trusted volunteer. Since this shelter was always full, I advised her to offer to foster the animal. Many shelters will happily send animals home with fosters in order to free space in cramped shelters. They usually provide food, kennels, and toys.

She drove back to the shelter and commented to a head employee that the place seemed more crowded than usual. She then asked what happens when they have no room for more animals. The employee explained the foster program and advised that they would reach out to fosters on file and beg for help. My client jumped on that opening and stated that she desired to be a foster. Of course, there was another application for that, but the employee did not ask for ID since my client was a registered volunteer with a record on file at the shelter. My client took her future dog home that day.

This was a big achievement. The dog was in her house. The shelter only knows my client by an alias name, and they know her true address. I advised her to do her job for a few days, enjoy the bonding, and ensure that the dog was a good fit. During her next volunteer assignment on a weekend when specific staff were present (the staff that she had bonded with the most), she advised them that she would like to adopt the dog she was fostering. This immediately presented the adoption application, which she completed with her alias name. The employee asked for an ID, which my client stated "I don't have it today, but I can bring it on Tuesday when we go to the Adoption Event". This was fine with the employee, and the rest of the application was executed. My client now owned the dog. At the next volunteer event, which was located at a local pet supply chain, the day was too busy for anyone to remember to obtain a copy of her ID. To this day, she still volunteers at the shelter, and no one has ever mentioned a need to copy her ID.

You may be reading this in disgust. I have encouraged a client to lie to an animal shelter. I can only offer the following. She hurt no one. She is an amazing and loving dog owner. Without the ability to stay private, she would not have obtained a pet from a shelter. Her actions were not in vain. The following events have occurred to her since the adoption:

- She has received over a dozen pieces of unsolicited mail at her home address in the name of the alias she only used with the shelter. These continue to expand as these companies share data with partner organizations.
- The email address that she provided on the adoption application now receives pet related spam daily. Advertisements for insurance, vaccinations, food, and safety gadgets flood that account, which she no longer checks.
- The telephone number she provided on the application was shared with a local veterinarian which has added it to a SMS text campaign. Every week, she receives unsolicited tips and reminders to arrange for various pet services (at a cost of course). She can terminate that VOIP number or simply turn off notifications for it.
- Her alias name and address appear in a premium database owned by Experian, which is searchable by anyone. More details can be found at www.experian.com/small-business/pet-owners.jsp. My client is not concerned, as the entry is not associated with her real name.
- 24PetWatch has updated their records to include her alias name and address within their database, which is accessible to thousands of people including practically every veterinary office in the country. If someone were to scan her pet's microchip, a social engineering pretext to a veterinary office could yield her name and address. Therefore, I advised that she update the record again. This time, she should use her same alias name but change the address to the shelter's location. If the dog is lost, the shelter will be notified. They have her alias name, address, and number on file to contact her. While unlikely, this could prevent an advanced attack if someone identified her alias name and address (and dog).

The next hurdles will be ongoing "maintenance". Pets need continuous vaccines and licenses. When you obtain an animal from a shelter, the animal is almost always spayed or neutered, current on rabies and other vaccines, and "legal" in the county. Once you take possession, you are responsible for the continued medical care and licensing. Most counties in the United States have a legal requirement to maintain yearly rabies vaccinations. Part of this requirement is to register your pet with the county and pay a yearly fee when you provide proof of vaccination. Usually, your veterinarian will submit all of this for you as part of your visit for a rabies shot. You have a couple of options here, and I will list them in order of preference.

If you have already established yourself under an alias name with a local veterinarian, let them do the work. Show up for your yearly appointment, pay the fee for the visit and the vaccination, and pay the additional fee for them to file this with the county. They likely have rabies tags from the county on site and can issue your tag the same day. Part of this action will include them passing along your information to the county. To be fair, this will include your alias name and real address. If YOU sent this information to the county, it could be considered an illegal act. If THEY submit this data to the county, the act is a little less grey. Only you can decide if this is appropriate, but know that animal registration data is public record.

If you purchase and administer your own rabies and other vaccinations, you can submit any required paperwork to the county. The county is really only looking to enforce rabies vaccinations and is not likely on a data hunt about the owner of the pet. Do not lie on this form, as it is a government document. In my experience, placing the name of the animal in the line that is meant for your name suffices, as long as you also include the address, proof of vaccination, and the yearly fee. In that case, you have not provided false information, you simply excluded your name and instead provided that pet's name.

You may be shaking your head at this, but it matters if you have a need to stay truly private. In 2017, I had a client with a crazy stalker who knew everything about her. She relocated into an anonymous home, but obviously kept her pet. The crazy stalker contacted animal control in the county where he suspected she was staying, stated that he found a dog with a collar and tag with a very specific name, and hoped to return the animal. The county found only two pets on file with that unique name and provided the address for both of them. One was my client. It only takes a small mistake to ruin all of your hard work.

Another hurdle is boarding an animal. I am lucky that I have a trusted neighbor who takes my dog in when I travel. He has twelve acres of fenced land and Riley runs with his dogs the entire time I am gone. However, I have had to board him once when the neighbor was unavailable. Gone are the days of dropping off the dog, leaving some cash, and picking it up later without many questions. Practically every professional boarding company will want proof of vaccines, veterinary records, and your personal information.

I chose a local outfit which had great reviews and visited it with Riley. Since it was my first time there, I had to complete an application and sign consent allowing the sharing of any data to third-party entities. It is almost impossible to escape this throughout our daily grind. I provided my alias name and an alias hotel address. I keep redacted copies of Riley's records for events such as this, and they accepted that as proof of rabies, Bordetella, and other vaccines. I purposely redact the name and address of the vet, as that should never be shared. That did not fly in this scenario. They demanded to know the name of the vet and stated that they would contact the office to obtain their own copies of Riley's records.

The problem here was that my vet does not know the name Riley and possesses yet another alias address. Since the vet office did not obtain my record from the shelter, they do not have my real home address. This can become difficult to manage quickly. Thinking as fast as I could, I provided my veterinary office information and told her that Riley is likely listed under Kosmo. I blamed this inaccuracy on me getting him from a shelter and they sent over the paperwork to the vet from when he entered the shelter. Not my perfect execution, but not too damaging either. She retrieved the records from the vet, including the alias address I had given them, and Riley entered a temporary home while I visited a client.

The outcome of this experience included several undesired communications. I received spam email messages from the boarding provider to my alias email provided to the veterinarian, which they obtained from the records sent over. I received unwanted SMS text messages on the burner number provided to them reminding me that they had new obedience classes. I probably received physical mail in my alias name at the random hotel addresses provided to the vet and the boarding service. I anticipated that my contact information would eventually be leaked to other related companies. When it did, there was not much concern, as they did not have my name and true address. In 2020, I received an email from a previously unknown vet in the same city as the boarder. The email confirmed Riley was due for updated vaccinations, as determined by the records sold to this vet by the boarder, which were copied from my original vet. Animals have no privacy either.

For the record, I no longer use boarders, as I find having close relationships with friendly neighbors with dogs is much more beneficial. They don't ask questions, demand ID, or want to see vet records. My dog is much happier when I return, and I have found that a surprise 50-pound bag of the neighbor's desired dog food left on his porch enables future stays.

In 2020, I encountered a new privacy issue in regard to pet care. My dog needed an expensive long-term prescription which is also available for humans. My vet encouraged me to have the prescription filled at Walmart, as it would be much cheaper. After learning the substantial price difference from an expensive pet brand medication versus a generic option from Walmart, I was convinced to take the prescription and have it filled on my own. Walmart agreed to fill the prescription within the local store's pharmacy, but demanded to photocopy my government-issued photo identification. I walked out empty-handed. However, Walmart, Chewy, and other providers offer online prescription orders with delivery directly to you. Identification is not required for online prescriptions, aliases can be used, and private forms of payment are accepted. However, there are other issues. The following happened to my client mentioned previously in this chapter.

Her vet directed her to a third-party supplier called VetSource for her monthly medications required for her pet. The vet even provided a discount code in order to save money on the first order. She went to the site, added her medications to the cart, and proceeded to check out. The service already knew the identity of her vet since she used a referral link from the vet's website, and VetSource informed her that they would need to verify her prescription with the vet before the order could be placed. She had used an alias name and true address with the Vet, but intended to use her real name and credit card for medications which would be shipped to a UPS box. She felt stuck. Any name and address on this order would be shared with her vet, and the order would probably be declined. In this scenario, she decided to use her real address and alias name for the order. The vet already knew this address since the adoption records displayed it. The vet confirmed the order and quarterly packages arrive automatically, being charged to a Privacy.com account.

I present this situation as the reason we must always have a solid plan before executing any privacy strategies. During the first visit to the vet, know the name and address which you will be using. This will be on file forever. If you need to have home deliveries of medication or the ability of home visits, plan for that. For most clients, I recommend providing an alias name, actual home address, and a masked form of payment. This can be a service such as Privacy.com or a prepaid credit card. Personally, I keep a prepaid Visa for use only with my vet. There are many benefits of your pet publicly belonging to your true home address. If he or she is lost, return can be made quickly. This also serves as some decent disinformation, as explained in a later chapter.

In most situations where you are obtaining any type of in-person service for your dog, cash payment should be acceptable. I never use a personal credit card, even a secondary alias card, for anything associated with my dog. You may still be wondering why my dog has alias names. It was unintentional at first. When I adopted my dog, he had a temporary name of Lightning. This was given to him when he arrived at the shelter because no one knew his real name and he was a bit wild. When I adopted him, I had no reason to advise the shelter that I would not be using that name, especially since he did not respond in any way to it, and that I had started calling him Riley. To this day, the shelter believes his name is Lightning.

Out of paranoia, I did not choose a veterinarian from the suggested list provided at the adoption. I sought my own option and took "Riley/Lightning" in for the next round of vaccinations and a checkup. On the new patient application, I provided the name as Kosmo. I don't know why. It just happened. I guess it is just habit. I was not using my real name, why expose his? I projected feelings of approval for this behavior from Riley, and my vet calls him Kosmo to this day. This was all fine, until it wasn't.

While at a local dog park, I encountered an employee from the shelter where I obtained Riley. We talked briefly while our dogs played, and then my vet showed up. He asked how Kosmo was doing, which seemed to surprise the shelter employee who had been calling him Lightning for the past 30 minutes without any correction from me. In an awkward tone, I called out "Let's go Riley!", and we left, likely adding more confusion. Maybe an alias for a dog is overkill.

This brings up another consideration. What information do you place on a pet tag? In previous years, I would say it really does not matter. Today, I have a firm opinion on this. I believe a pet tag should only have one piece of information on it. It should only include a reliable telephone number which can reach you at all times. I use a MySudo number for this, but you may have other VOIP options. Most tags have a pet name, owner name, address, phone number, and email. The following explains my reasons to exclude most of these details.

- Pet name: Why is this necessary? Will that determine whether a person that found your animal will call you? I do not believe so. This also prevents you from ever giving some stranger a wrong name for your pet.
- Owner name: This one is obvious. Any name I provide would be fake anyway. Anyone that finds my pet will not know me. Again, this locks you into a specific alias name when you are out with your animal.
- Address: If you are comfortable with exposing your home address without a name, this is not a huge issue. My reservation is during the creation of the tag. You have likely seen machines at pet stores which allow you to create your own custom tag. These are very affordable and provide an immediate result. They also share those details with affiliate companies. Think about the potential. If you owned thousands of machines in big pet stores that made pet tags, and you obtained the names, addresses, and phone numbers of the owners, you would have some valuable data. Pet supply and insurance companies devour this data and bombard users with unsolicited offers. I do not want to share my home address, regardless of alias name.
- Email: Aside from the previous reason, email addresses are more prone to spam. I also suspect that anyone who found my pet would rather call and may not bother sending an email. Additionally, burner email addresses could expire when not used and you may not receive the message. You are also trusting the ability to avoid typos from the finder.

For these reasons, my dog's tag has only a telephone number. I find that to be sufficient. Do you need to provide an alias name to associate with your pet(s)? Only you can answer that. I only hope that this chapter has provided some insight from my experiences, and exposes the data leakage that happens when you possess an animal. My final thought to close this chapter is that numerous entities want a piece of the action in regard to your pet. Pay the legally required licensing (county/city fees), provide the legally required care (rabies and other immunizations), and stay out of scope from anyone tasked with holding people accountable. Play by the rules, but never provide more personal details than necessary. Surprisingly, minimal information disclosure is required, but we tend to give in to marketing tricks.

Chapter Thirteen

Beyond Extreme

You may believe that the privacy strategies presented in this book are a bit too complex for your needs. For many of my clients, the previous pages represent only the basics, and there is a desire for the next level of privacy. Some clients need extreme protection through name changes, dual citizenships, or various uncommon legal documents. Most people reading this may need none of that. However, in the rare situation where you are targeted by a powerful adversary, these are tools to possess in your arsenal of privacy strategies. Before proceeding, let's have a quick sanity check and consider your progress.

Until now, I have focused on the most popular services which my clients request from me. Moving to an invisible home, driving an anonymous car, and communicating from sanitized electronics are very normal in my business. These are the things which I encourage you to implement. Changing your name, moving to another country, giving birth to expedite citizenship, and planning the details after your death are rare, but I have assisted in these situations. This chapter represents the extreme of the extreme. Please do not execute any of these strategies without seriously considering all potential consequences. Of everything discussed in this book, the methods explained in this chapter backfire the most. For many, this content may just be an entertainment break before jumping back into common strategies. For others, it may save their lives.

Readers of the previous edition of this book offered criticism of the placement of this chapter. Many believed it should have been presented at the very end of the book. This is valid feedback, but I chose to leave it in the current chapter lineup. This chapter navigates us toward the end of our PROACTIVE journey toward extreme privacy. In the next chapter, I transition to methods for damage control, which are more defined as REACTIVE. Afterward, I present two entirely new chapters about physical privacy and advanced technology strategies. You may be tempted to skip this chapter and move on to more applicable topics. The content within this chapter is not necessary in order to implement later tutorials. However, I hope that you will indulge me by considering the topics presented within the next several pages. If you ever find yourself stuck within an exceptionally rare threat, you may need to rely on these extreme methods.

Name Change

For the record, I almost never recommend a name change (outside of a traditional change associated with marriage or adoption). Changing your name does not carry the power it once had in previous decades. Today, your new name is likely to appear as an alias on your consumer profiles within data mining products. This is because your new name is still associated with your current SSN. Additionally, some states and counties require your name change to be publicly posted, such as within a local newspaper. Digitization and permanent archiving of these details will not keep them hidden long. For clients who are insistent on a name change, I follow a specific recipe.

First, I run them through the nomad residency process through South Dakota as previously explained. I obtain a new license in their official name, and then wait. Six months after residency, you are allowed to petition for a name change. The required forms can be found on the South Dakota website at https://ujs.sd.gov/Forms/namechange.aspx. The process begins with a petition for change of name, followed by a hearing, and finally an order if the change was approved by a judge. All of this will require physical presence within the state and multiple court visits over the period of a couple of months.

This process is very similar in other states. The difference is the privacy. Many states, such as California and New York, make court records public on the internet. This is becoming the default action as most states digitize all historic records and place them online. Some more populated states allow third-party companies to devour this data electronically via application programming interfaces (APIs). In other words, many states allow companies to automatically suck up all court documents in order to populate their own data mining systems. South Dakota is much more reserved. While a name change is public record, unless a judge can be convinced it should be sealed, South Dakota does not go out of their way to notify the world. In my experience, it is not difficult to convince the court that a name change should be sealed (private) in scenarios involving physical attacks toward the victim. This will not make you invisible as your true privacy threat is your SSN and DOB combination.

If you are going to change your name for privacy reasons, you really need a new SSN in order to stop the association. Even then, it will be easy for companies to determine you are the same person. Changing your SSN requires a visit to a Social Security office. You will be required to show ample identity documentation and your current Social Security card. This is not an immediate process, and your old number will remain present within many systems. Your case will be evaluated, and a new number may be denied. If issued a new number, expect problems with any attempts to establish new credit. If you do require a new credit card or loan, the new SSN and the old will be permanently connected, which removes any privacy strategy here.

Overall, I do not recommend name changes and/or a new SSN. In order to possess any privacy, you can never obtain any new credit or use your new name and SSN on any official documentation. This will be difficult. If you slip, you associate the old information with the new. I believe that you can achieve the same level of privacy by executing the previous methods displayed throughout the book. With permission, I provide the following undesired result after a name change was conducted for a client.

In 2019, "Janis Doe" had become a South Dakota nomad. Her PMB was the only valid address on any public or private record. Her condo was in the name of a trust and her vehicle titled to an LLC. Her utility companies had no clue of the identity of the occupants in her home. In my opinion, she was invisible. She contacted me with a desire to change her name as a final strategy to eliminate her past. After encouraging her to avoid a name change, she insisted on moving forward and I began the process.

We submitted the paperwork with the state and she made her appearances in front of a judge. Due to her experiences with physical abuse, the court agreed to seal the record. Within a few weeks, she was now "Janis Smith". She obtained a new driver's license in this name, applied for a new passport, and she now had a new identity. Eventually, the Social Security Administration confirmed they recognized the change but delayed issue of a new SSN. That is when the real problems began.

When she notified her bank of the name change, they insisted on sending a physical form which would need a "wet" signature and notary. She provided her PMB address which was flagged as a CMRA mail drop. The bank refused to send anything to that location. Since they wanted to verify a physical address, stopping by a local branch would not help. Until she provided her true physical address the bank refused to update her information. After a few visits to a local branch, a manager finally agreed to file the paperwork on her behalf. This was the beginning of the paper trail which would ruin her efforts. Her insurance policies, credit cards, and retirement accounts were all updated, and each of them added to the trail. As I write this in 2020, a search of this "Janis Smith" within every premium data mining company to which I have access reveals her to have an "also known as (AKA)" entry for Janis Doe. A search of her old SSN immediately connects to a record of the new SSN. The two identities are very connected and she has no real privacy protection from the name change.

Today, I believe there is no reason to change your name or SSN, aside from emotional scars from family issues. These changes will not erase your financial, residential, and family past, and will always leave a trail which combines the two identities. The name changes of fifty years ago were effective. Today, they are just cosmetic.

Marriage Considerations

The physical location of your marriage can have a huge impact on your privacy. Consider two states which approach public access to this type of information very differently. New York provides public access to all records via a dedicated division titled the Vital Records Office at the New York State Department of Health. Their website proudly announces that every marriage (and divorce) record from 1880 to present is available to anyone online. A simple search form is provided for immediate access. In contrast, Colorado's state law (C.R.S. 25-2-117) declares vital records such as birth, death, adoption, marriage, and divorce as confidential. As a result, Colorado vital records are not public records; therefore, they are not searchable online. Vital records can only be released to those who are eligible, such as the bride, groom, or an immediate family member. These are only two examples. You should research the laws and policies of any state where you are considering marriage.

If you had your mind set on a California wedding, you have a surprisingly private option. California is the only state which offers both a regular public marriage license and a confidential marriage license. A confidential marriage license is legally binding but not part of any public record. Section 501 of California's Family Code allows the county clerk to issue this option. Section 511 states that these licenses are not open to public inspection except by a court order. However, public marriage licenses allow anyone to look at the personal information that appears on the licenses at the county clerk's office. This includes the couple's names, dates and places of birth, parents' names, and any previous marriages.

I have been asked on several occasions whether a confidential California license is better than a public license from within a state which does not allow online search of marriage records. In most scenarios, I believe the California confidential option is better. If a state which is fairly private now, such as Colorado, later changes to a public record model, your details could become publicly shared with third parties. I believe this is less likely with an intentionally confidential license from California. Many states offer an option to have the court seal the record, but this brings unwanted attention to you, and you will be forced to convince a judge to protect your privacy. I prefer more streamlined options.

Overall, I recommend that privacy-seeking clients apply for a marriage license, and execute the ceremony, outside of their home state. This provides a small layer of privacy. Many automated people search databases will associate marriage records from within a specific county to people with those names from that county. Marriage records from distant counties may not be automatically added to a person's profile. However, if the public marriage record includes dates of birth and parental details, it will likely be associated with the individuals anyway. This is why I push clients to become married in states which respect the privacy of the marriage, and are at least one state away from their home. Always contact the county of potential marriage to identify whether the details are publicly shared.

The next consideration is name changes due to marriage. In the United States, it has been customary for the bride to take the surname of the groom. I believe this is very traditional thinking which has not kept up with our current society. Today, it is very common for each spouse, regardless of gender, to keep their own surname. In most scenarios, I believe this is best. It is not only convenient to avoid countless name change forms, but it also provides two last names which the couple can use when necessary. Consider the following scenarios.

- A spouse with a very unique name is heavily targeted with online threats. The spouse with a common last name can hide more easily within online records if the name should become public after utility or delivery details become public.
- The same targeted spouse feels uncomfortable associating his last name with the couple's new home, but the HOA demands a confirmed resident be listed within the neighborhood records. The spouse with the more common name, who is not targeted, could be included in the documentation, with less threat.
- In contrast, a spouse who is being heavily targeted could decide to take the last name of the spouse with a more common name in order to provide a slight layer of privacy.

In each of these scenarios, the protection is minor, and does not replace the privacy strategies explained throughout the book. If executed properly, your name(s) will never be associated with your home, and none of this may matter. However, backup plans are always nice. Next, consider the privacy invasions of online wedding registries. These require you to publicly disclose the names, location, and general details of your upcoming wedding and attendees. This information is later sold to other companies in the wedding industry. You are also required to disclose a physical address to which your gifts can be shipped. I encourage you to eliminate this marketing scam from your wedding. Your family and attendees will likely revert to the old-fashioned gift-giving methods from a pre-internet era.

Sanity Check: Modifying the plans of your marriage may present a new layer of privacy desired by you. However, consider the feelings of your spouse. Refusing to take a married name (or refusing to give it) could create serious strain on a new marriage. Hiding the details from public view may generate a suspicion of embarrassment in the relationship. Never execute these strategies without seriously discussing it with your partner. If there is hesitancy or a sense of confusion and discomfort, take a step back and identify the issues. For me as well as my clients, family relationships are more important than the desire to disappear. If your partner is on board with all of this extra effort, you may have found your match. Approach cautiously and do not blame me when you are left at the altar because you did not consider the wishes of your mate.

Birth Considerations

Many childrens' birth certificates are public record. While we do not see them copied into people search websites, the data itself can be usually seen or verified by anyone willing to visit the county seat and claim to have a need for a copy of the record. Worse, services such as VitalChek (a LexisNexis company), allow practically anyone to order another person's birth certificate online by confirming a relationship and need. While writing this section, I provided publicly available information about myself to VitalChek. I stated I was a relative and the service authorized me to obtain my own birth certificate as a genealogy researcher. The cost was $20 and anyone could have replicated this by knowing only my name, date of birth, and mother's maiden name. All of these details can be found online about most of us.

Similar to marriage records, states such as California make birth certificates easily available to data mining companies while states such as Colorado consider them confidential. Let's consider the data required to complete a birth certificate which could become public. Most states require the following information, which is usually submitted by a medical attendant.

Child's Name	Location of Birth	Parents' Places of Birth
Child's Gender	Parents' Names	Parents' Signatures
Child's Date of Birth	Parents' Dates of Birth	

This information may not seem too sensitive to most. A home address is usually not present unless the birth occurred at home. However, I respect that some clients do not want these details released publicly. Some may be keeping a relationship secret, while others do not want any clues about the county in which they reside available to a stalker. Regardless of your situation, extreme privacy enthusiasts may desire to keep a birth certificate private. Some states have specific laws which declare birth certificates confidential and only available to immediate family. However, I find this to be a small hurdle to bypass. While illegal to access someone else's birth certificate without family authority, people do it anyway. I encourage clients in extreme situations to assume that the birth certificate for their child will become public record. Therefore, they should consider the key data which will populate the document.

Location: If I know the county in which you live, I know where to search for a birth certificate. If you choose to give birth in another county, this makes my search more difficult.

Name: If I know the name of your child, possibly if it were posted to social media, I would have enough information to conduct a search. Preventing details of your birth from appearing on the internet eliminates the easiest way to obtain a copy of the birth certificate.

While we are discussing names, we should address privacy implications of naming a child. The less unique his or her name is, the greater your child's privacy will be in the future. A person

named John Smith may be much more difficult to track than one named Michael Bazzell. Finding the right John Smith would require substantial time to sort through thousands of records. If you have a common last name, you are already at a huge advantage over those who have unique surnames. There are still steps you can take to make your child less distinguishable. While I respect that passing a family name to a child is a traditional and important piece of family history, there are extreme situations when this may be avoided. I have witnessed the following.

- Some privacy enthusiasts will choose the desired name with which they wish to address their child, but make it the middle name. If they desire to call their child Michael Bazzell, they might make the official name John Michael Bazzell. This results in most people search sites identifying the child as John Bazzell. People who know him as Michael Bazzell might not identify this association.
- In one scenario, a couple did not possess the same last name. They were married, but the wife never changed her name to match the husband. They decided to "mash-up" their last names and provide their son a unique last name. Assume the father's last name was Bazzell and the mother's name was Singleton, the child's last name was similar to Baton. Obviously, this is a fictional example in order to protect the privacy of the real parents and child.
- Some choose to issue numerous middle names to a child. John Michael William Bazzell could legally use John, Michael, Mike, William, Bill, Billy, or Will as a legal name at any time. This provides numerous legal aliases ready for the future.

The next consideration is the Newborn Genetic Screening test, which is required in all 50 states. Nearly every baby born in the United States gets a heel prick shortly after birth. Their blood fills six spots on a special paper card. It is used to test for dozens of congenital disorders which, if treated early enough, could prevent severe disabilities and even death. Some states destroy the blood spots after a year. However, many states store them for at least 21 years. California is one of a few states which stores the blood spots for research indefinitely. These results are often given to researchers, queried by other government agencies, and sold to private corporations. You pay the fees for this mandated test.

Most hospitals provide information about this data collection and your rights according to the specific state where the child was born. Most states require submission of a card which either allows consent to share the data collected or explicit refusal to participate in the program. Some parents may choose to omit their child's blood sample from any state or national databases. Many people report that the samples are collected and shared if no action is taken after birth. I encourage you to identify this consent form and consider your options.

It desired, notify the hospital that you do not want a birth announcement in the local newspaper. A surprising number of hospitals provide this data without parental consent.

Death Considerations

Let's get gloomy. We are all going to die. For some, our privacy shenanigans may not matter after we are gone. For others, including myself, our death may be the opportunity to apply one final privacy strategy. Most of my clients are not concerned with keeping death details private, but we should all consider our families' needs once we leave. Anything we can do now to ease the decisions surrounding our passing will be welcomed by those faced with the responsibility. Let's start with some additional documentation which may be helpful.

Final Arrangements Document

Most states do not have any specific laws about the validity of a Final Arrangements Document, also known as an End of Life plan, Final Wishes Planner, or combination of any of these terms. Typically, this is a document outlining your final desires related to your funeral, public death announcements, disposition of your body, and service details. This may not be considered a legal document, but it can be extremely helpful to those planning your funeral and death announcements. First, let's consider why we may desire such a document.

People search websites scrape online obituaries for deceased family member's details. They then populate the newly discovered data into their invasive systems. Consider the following demonstration. You are a very private person and your mother passes. A traditional obituary will publicly display your full name, spouse's name, actual city of residence, children's names, and relationships to all siblings, nieces, nephews, etc. People search websites devour this data and append your profile. Within weeks, you are listed within dozens of websites which accurately identify your location and family members. If this bothers you, a Final Arrangements Document can protect your relatives when you pass.

Please note this document is not publicly filed with any government entity. A Notary signature is not required, but witness signatures are vital. I also encourage you to explain this document and your wishes to immediate family. You do not want someone challenging the validity of this document. I have witnessed funerals which were conducted in a completely opposite manner as the deceased intended due to arguments among the children.

The following page presents a sample document with fictional information. This can be modified in any way desired to meet your own demands. I present this only as a guide. For some, this may remain a single-page directive. Others may incorporate elaborate details. Most readers will rely on this document in order to prevent personal details from being shared publicly through death announcements and obituaries. It also specifically outlines a desire to prevent personal information from being shared through social networks.

Final Arrangements Document for John Wilson

I, John Wilson, currently of Los Angeles, CA, being of sound mind, willfully and voluntarily declare that these are my final wishes as to the disposition of my body after my death and any services or memorialization to be held in my name. This document is not intended to be interpreted as my Last Will and Testament.

APPOINTEE: I request that Jane Wilson be in charge of executing my last wishes.

DEATH ANNOUNCEMENT: I wish to have a death notice submitted only to the LA Times. My death notice should include my date of birth as January 1, 1980 and my birthplace as Los Angeles. It should not include the names or locations of any family members as respect toward their privacy. I do not wish any details of my funeral or other services be included in my death notice. I request my death notice to exclude any residential, hobby, or employment history. I request that any death announcements be omitted from any social networks or online forums, including, but not limited to, Facebook, Twitter, Instagram, and Snapchat.

ORGAN DONATION: I wish to donate my organs upon death and am a registered organ donor in the state of California.

DISPOSITION OF BODY: Upon my death, I wish my body to be cremated. I wish for my ashes to be scattered as desired by Jane Wilson.

SERVICES: Upon my death, I wish to have a private memorial service to commemorate my life. I would like it to be held at the Elks Lodge, located in Torrance, California, if possible.

FINANCING & EXECUTION: I have set aside funds to cover my expenses which are located in my safe. I request that Jane Wilson follow the spirit of these wishes as well as she can and within the limits of any applicable law.

_____ _____

John Wilson Date

_____ _____

Witness Name Witness Name

_____ _____

Witness Signature Witness Signature

_____ _____

Date Date

Living Will (Instructions for Health Care)

A Living Will does not outline your desires for distribution of assets after you die. Instead, it is a legal document which explains medical directives while you are alive. This document likely exceeds the scope of this book, and has very little relationship to privacy. However, it fits well within this section and can provide value to those already making end of life decisions. First, consider a few reasons why you may need a Living Will.

It Protects You When You Cannot Communicate: The biggest advantage of having a Living Will is that it protects you in a future situation during which you no longer can communicate your wishes. Otherwise, medical professionals in charge of treating you have the authority to choose your treatment on your behalf once you are in a state in which you cannot communicate what you want to be done.

It Prevents Arguments Between Family Members: Medical care decisions can cause a lot of trouble among family members. If they disagree on what should be done, it can cause relationship-ending arguments. With a Living Will, it will be your choice and no one else's. This should help eliminate any argument or debate as to what should happen to you.

It Gives You Control Over Medical Treatments: A Living Will provides you complete authority over which medical treatments and procedures take place in a situation where you are unable to communicate. In this specific situation, a Living Will legally demands doctors to fulfill your wishes and removes the decision from them.

It Reduces Potentially Unwanted Medical Bills for Your Family: In the situation that you get into a coma or vegetative state, a Living Will determines healthcare action. Some people would rather die than live an additional 20 years on life-support. This is usually due to the enormous medical bills for which their family will have to pay while you are miserable. If you do not want to see something like this happen, you need a Living Will that specifies exactly what you would like to happen in a given situation.

It Provides Peace of Mind: Finally, Living Wills are designed to give you the control to prevent more bad things from happening in already tragic situations. You may want to know that your family, as well as yourself, will be taken care of properly in such a situation.

I encourage you to be proactive while considering your desires for end of life decisions. Don't surrender control over what happens to you under bad circumstances. The following document contains the basic language of a Living Will. You can also find numerous templates online which contain more detailed information. Choose a document most appropriate for your desires.

INSTRUCTIONS FOR HEALTH CARE

END-OF-LIFE DECISIONS: I direct that my health care providers and others involved in my care provide, withhold, or withdraw treatment in accordance with the following:

__ Choice Not To Prolong Life: I do not want my life to be prolonged if (i) I have an incurable and irreversible condition that will result in my death in a relatively short time, (ii) I become unconscious and, to a reasonable degree medical certainty, I will not regain consciousness or (iii) the likely risks and burdens of treatment could outweigh the expected benefits, OR

__ Choice To Prolong Life: I want my life to be prolonged as long as possible within the limits of generally accepted health-care standards.

ARTIFICIAL NUTRITION AND HYDRATION: If I have selected the above choice NOT to prolong life under specified conditions, I also specify that I _____ do or _____ do not want artificial nutrition and hydration provided to me.

RELIEF FROM PAIN: I direct that treatment for easing pain or discomfort be provided at all times, even if it hastens my death.

EFFECT OF COPY: A copy of this form has the same effect as the original.

REVOCATION: I understand that I may revoke this OPTIONAL ADVANCE HEALTH CARE DIRECTIVE at any time, and that if I revoke it, I should promptly notify my supervising health-care provider and any health-care institution where I am receiving care and any others to whom I have given copies of this document. I understand that I may revoke the designation of an agent only by a signed writing or by personally informing the supervising health-care provider.

_____	_____
John Wilson	Date

WITNESSES:

_____	_____
Witness Name	Witness Name
_____	_____
Witness Signature	Witness Signature
_____	_____
Date	Date

Traditional Will

In previous chapters, I explained the privacy strategies when using a trust to hold assets. During the discussion about Living Trusts, I explained that they have more power than a traditional Will because a trust does not go through probate. However, I do believe that everyone should also possess a traditional Will. It can be a "catch-all" document to address any concerns with assets which were not included in any trust.

A traditional Will does not necessarily offer much privacy benefit. My goal within this section is to identify additional unconventional details which can be beneficial to a privacy enthusiast. While a Will should not become public information, you should be cautious of its contents. During the probate process, practically anyone can claim they should be able to see the Will in order to potentially protest the validity. This is not common, especially with close families, but something we should consider. I have never seen the details of a Will become part of a people search site, so we can (and should) include family member details.

The following two pages include common language used within a Will. You should consult an attorney before executing your own Will, especially if you possess substantial assets. In order to keep within the scope of this book, I will only emphasize the items included in section (7) titled Special Requests. This area allows you to enter any details which would normally be absent from a Will. Since this is a legal document, as defined by the Will laws of your state, it may hold more power than any previous documents we have created. Specifically, consider my reason for including the following items.

(7.1) I direct that my Final Arrangements Document be executed upon my death.
(7.2) I direct that details of this document are not to be shared publicly or online.

The first item (7.1) provides some legal coverage for the Final Arrangements Document we previously created. This is likely not necessary, but may give cooperating family members leverage over those who wish to defy your desires within that document. The second option (7.2) is fairly vague and may have no consequences if ignored. However, having your desires to keep this information private, while visible to the entire listing of beneficiaries, may ensure that your requests are executed properly.

Some may question the need for a separate Final Arrangements Document, which was explained previously as a way to handle your funeral and public details, instead of simply including those details within a traditional Will. There are two reasons a single document is inappropriate. First, a Will is often viewed and executed weeks or months after death. The details are often ignored until after the funeral, which eliminates any chance of the end of life desires being granted. Second, a Will must go through probate and can be contested. I believe these documents should be separate.

LAST WILL AND TESTAMENT of JOHN WILSON

(1) Declaration: I hereby declare that this is my last Will and testament and that I hereby revoke, cancel and annul all Wills previously made by me. I declare that I am of legal age to make this Will and of sound mind and that this last Will and testament expresses my wishes without undue influence or duress.

(2) Family Details: I am married to JANE WILSON, hereinafter referred to as my spouse.

(3) Appointment of Executors:

(3.1) I hereby nominate, constitute and appoint JANE WILSON (SPOUSE) as Executor or if this Executor is unable or unwilling to serve then I appoint MICHAEL WILSON (SON) as alternate Executor.

(3.2) I hereby give and grant the Executor all powers and authority as are required or allowed in law, and especially that of assumption.

(3.3) Pending the distribution of my estate, my Executors shall have authority to carry on any business, venture or partnership in which I may have any interest at the time of my death. My Executors shall have full and absolute power in his/her discretion to insure, repair, improve or to sell all or any assets of my estate. My Executors shall have authority to engage the services of attorneys, accountants and other advisors as he/she may deem necessary to assist with the execution of this last Will and testament and to pay reasonable compensation for their services from my estate.

(4) Bequests: I leave my entire estate to my spouse, JANE WILSON.

(5) Remaining Property and Residual Estate: I bequeath the remainder of my estate, property and effects, whether movable or immovable, wheresoever situated and of whatsoever nature to my spouse JANE WILSON.

(6) Alternate Beneficiaries: Should my spouse not survive me by thirty (30) days then I bequeath the remainder of my estate, property and effects, whether movable or immovable, wheresoever situated and of whatsoever nature to:

Name: MICHAEL WILSON (SON)
Bequest: 50% of remaining estate.

Name: AMY WILSON (DAUGHTER)
Bequest: 50% of remaining estate.

(6.1) Should any of the beneficiaries named in (6) not survive me by 30 (thirty) days I direct that the non-surviving person's share goes to the remaining beneficiary.

(7) Special Requests:

(7.1) I direct that my Final Arrangements Document be executed upon my death.
(7.2) I direct that details of this document are not to be shared publicly or online.

(8) General:

(8.1) Words signifying one gender shall include the others and words signifying the singular shall include the plural and vice versa where appropriate.
(8.2) Should any provision of this Will be judged by an appropriate court of law as invalid it shall not affect any of the remaining provisions whatsoever.
(8.3) If any beneficiary under this Will contests or attacks any of its provisions, any share or interest in my estate given to that contesting beneficiary is revoked and shall be disposed of in the same manner provided herein as if that contesting beneficiary had predeceased me.
(8.4) This document shall be governed by the laws in the State of California.

IN WITNESS WHEREOF I hereby set my hand on this 7th day of July, 2020 in the presence of the undersigned witnesses.

_____
JOHN WILSON

As witnesses we declare that we are of sound mind and of legal age to witness a Will and that to the best of our knowledge JOHN WILSON is of legal age to make a Will, appears to be of sound mind and signed this Will willingly and free of undue influence or duress. We declare that he signed this Will in our presence as we signed as witnesses in the presence of each other, all being present at the same time. Under penalty of perjury we declare these statements to be true and correct on this 7th day of July 2020.

_____	_____
Witness Name	Witness Name
_____	_____
Witness Signature	Witness Signature
_____	_____
Date	Date

After-Death Data Access

The final consideration in regard to death is the accessibility of your data. When you die, the passwords known only to you die. This may eliminate the ability to access your documents, media, accounts, communications, and anything else you have protected. For some, this may be intentional. You may not want anyone to be able to access this information, even after your death. For others, it is vital to allow a spouse or other family member complete access to your digital life. Imagine that you control all of the online accounts related to your house, banks, utilities, and aliases within a password manager. You die and your spouse cannot access these details in order to continue payments and maintain your privacy strategy. This can be devastating, especially if nothing is in your true family name. For most clients, I recommend an after-death data access strategy. If you created any of the documents previously discussed in this chapter, you should attach a separate document explaining any components of your privacy strategy which would be needed after your death. This should include the following.

- Passwords required to access any online accounts associated with your home.
- Detailed alias names used for any services or utilities associated with your home.
- Detailed payment processes for any services or utilities associated with your home.
- Detailed access instructions for any financial accounts.
- Detailed access instructions for secured containers (safes).
- Detailed access instructions for any virtual currencies stored digitally.
- Copies of any Trusts, Wills, and financial records.

These are only a few considerations. Consider what information will be needed when you die. Making this content easily available may seem risky. What if this data gets into the wrong hands? This is a very valid concern. You should be creative and cautious in how you disseminate these details. Some may include written information in the same envelope as their legal documents within a safe. I take it to another extreme.

I created a text document which includes every detail needed to reconstruct my complicated digital life and understand my use of aliases, trusts, and LLCs. It is encrypted within a VeraCrypt container and copied onto USB devices held by my two beneficiaries. My attorney possesses a password which is to be given to each beneficiary only upon my death. The beneficiary can use that password, followed by the serial number of the USB drive to unlock each VeraCrypt database. This way, the attorney has no access to the data, and each beneficiary requires cooperation of the attorney in order to access the content of the data they hold. Since each beneficiary has the ability to access the data without the other, there is a bit of redundancy in my plan in case one should lose the data or precede me in death. Every few years, I update the content on each USB drive in order to stay current. It makes for an awkward visit. I hope this page has generated some ideas on how you will tackle this dilemma.

Dual Citizenship

On rare occasions, I hear from a client that he or she wishes to obtain dual citizenship. This provides a second passport in your true name from a country outside of America. Dual citizenship is completely legal, but a huge hassle. There can be several legitimate reasons to desire a second passport from another country, but they are mostly obtained for the "cool" factor. If I were forced to identify legitimate needs for dual citizenship as an American, I would provide the following three reasons.

Travel: A second passport can protect you from travel controls and provide more visa-free travel. Visa-free travel is the ability to enter a country without obtaining a visa in advance. If you have a U.S. passport, you need to obtain a visa to travel to places such as China. This can become an expensive and time-consuming task if travel is frequent. If you had a passport from Grenada, a visa is not required to enter China from a country other than the U.S. These scenarios are rare, but legitimate for some.

Investments: Many countries refuse to allow Americans to invest within their territory. This is often due to strict American banking laws which requires citizens to report offshore accounts. Foreign banks simply do not want to deal with you or the IRS. A foreign passport can break through these barriers and allow investment. I do not get involved with clients in this situation. It almost always leads to some level of tax avoidance.

Safety: Having more than one option means you don't belong to a single government. If things become unsafe in America, and we find ourselves in danger simply being present, you can immediately and effectively take yourself and your family out of harm's way. While unlikely, options are always a good idea. My clients who desire a second passport usually fit mostly into this category.

There are three main strategies to obtain a second passport, which are ancestry, time, and money. All of my clients who have expressed interest in dual citizenship have chosen the easiest option, which is money. If you have enough of it, you can buy a passport from one or more of many countries. I have one client who collects them like baseball cards. Let's first take a look at the three avenues to dual citizenship, in order of most affordable to most expensive.

Ancestry

Obtaining a second passport usually requires either a lot of time or a lot of money. If you have the good fortune to have parents, grandparents, or in some cases, even great-grandparents from specific countries, a second citizenship can be easily and inexpensively obtained. If you have ancestors from Italy, Poland, Ireland, Germany, England, France, Portugal or Estonia, you might be entitled to citizenship based on ancestry. This means you can get a second passport in a very short time, and at very low cost. I always encourage clients to explore their family tree and identify any easy routes first.

Time

Most countries provide an option for naturalization through residency. However, the conditions vary with each country. Consider the following three factors.

- How long must you be a resident in order to be eligible to begin the application process for naturalization?
- How difficult is it to obtain residency? There are many countries eager to take in hard-working individuals, while others scrutinize and deny most applicants.
- Do you actually need to physically live there? Many countries' naturalization regulations require an applicant to spend the majority of time in that country. If you spend too much time out of the country, you render yourself ineligible for citizenship. Some countries have very minimal requirements for the length of time you must be physically in the country.

Money

Finally, the easiest option. If you have enough cash, you can often "buy" your dual residency. In previous decades, enough money would guarantee you a passport within weeks, without any investment or time requirements. In some rare cases, a $5,000 "donation" to the country generated a passport that same day. Those deals are no longer available, and the theatrics have changed. Countries now often require large investments while some still accept pure donations. As I present each country's options, I clearly display the outright fee you can pay in order to quickly bypass the lengthy application process for traditional naturalization.

Residency vs Citizenship

If you are not eligible for a second passport through ancestry, time, or money, the next best option is to obtain a second residency. It gives you the same benefit of always having a place to go, and it can potentially help you obtain a second passport within a few years through naturalization. Residency should not be confused with citizenship. Citizenship provides you an official passport which can be used for transportation. Residency simply grants you the authority to reside in the country. Residency is often a large role in the path toward citizenship.

The following pages explain the possibilities for obtaining a second citizenship for many of the countries which allow it. In order to avoid preference, or expose my own interests in this privacy strategy, I have listed them in alphabetical order. Please note that foreign politics change rapidly, and this information could become outdated quickly. While there may be additional countries which allow this and are not listed here, I present those which have a lengthy track record of positive experiences. There are many online scams surrounding "too good to be true" options which should be avoided. Each country summary ends with two considerations, as displayed below.

Cost: The average fee (USD) you will pay to obtain dual citizenship, instead of time.
Time: The amount of residency time required to apply for citizenship, instead of a fee.

Antigua and Barbuda

Antigua previously offered an affordable economic citizenship program, and recently reinstated it with much higher costs. There are now three options under Antigua's passport program.

- Pay $250,000 as a donation to the National Development Fund, as well as approximately $50,000 in legal and other fees.
- Purchase government-approved real estate valued at $400,000 or more, and hold that real estate for at least five years. You must also pay nearly $100,000 in legal and government fees per adult, and about $50,000 per child.
- Invest in a local business or businesses with a minimum investment of $1.5 million.

Cost: $300,000 or $1.5M investment **Time**: Not Applicable

Argentina

An Argentine passport allows visa-free travel throughout all of Europe, including Russia. However, Argentine passport holders must have a visa to enter the U.S., Canada, and Australia. Argentina's nationality law has been unchanged since 1869 and states that one can

qualify to become a citizen after only two years of residing in the country. Any residency visa qualifies you for this. Similar to Chile, the easiest options are "rentista" or retiree visas, which require you only to prove a certain amount of monthly passive income. In Argentina, in order to qualify for the rentista visa you need to demonstrate a minimum of $1,000 per month in passive income, which needs to be transferred to an Argentine bank account in your name. The rentista visa is a temporary one-year visa. It can be extended in one-year increments. It is best to initiate the residency process while in Argentina, not as a consulate abroad, which would complicate matters unnecessarily. Once you have your residency, you should spend at least six months of the year in Argentina for both years. After two years, you may apply for naturalization. Upon application you will need to demonstrate an intermediate level of Spanish language proficiency. The language test is very informal and "friendly", usually consisting of a short conversation.

Cost: Living expenses **Time**: 2 Years

Belgium

Belgian citizenship is quite valuable as a gateway to the European Union. It has some great options for first gaining residency, and once you become a resident you can apply for naturalization in 5 years. The most appropriate way to obtain residency in Belgium, and eventually citizenship, is to create a company in Belgium and apply for the professional card residency. You could also hire yourself from your company and apply for a work permit. This requires the services of a legal professional to assist you through the process. Obtain a residential address by renting or purchasing a home. Once you have the address, register it with the local city hall. Stay at that residence for the initial police check, which usually happens within two weeks and likely won't be repeated during the course of the visa. This makes you a resident of Belgium. After two years, apply for renewal, then renew every 5 years. You are eligible to apply for naturalization after five years. You can then go to the local municipality to state your intention of becoming a naturalized Belgian citizen. They will inform you of the documents necessary for application. In order to become naturalized, you do not need to physically live in Belgium full-time. The Belgian government has no way of knowing whether you are spending your time in bordering countries. However, you do need to spend a "reasonable" amount of time there each year and show that you are a member of the community.

Cost: Living expenses **Time**: 5 Years

Chile

A Chilean passport allows you to travel to 150 countries visa-free. It is one of only two travel documents that enables you to travel to all G8 countries visa-free. This includes the U.S.,

Canada, and Russia. It requires approximately five years of continuous residency, first temporary, followed by permanent residency. For individuals with established income and assets, the easiest option is called the rentista visa. To apply for this visa, you need to prove that you have income from investments held overseas. The easiest path for most clients is a lump-sum held within a bank account which pays interest. After nine months on the rentista visa, and having spent at least six months in Chile, you can apply for permanent residency. The six months do not need to be consecutive and can be accumulated over the course of one year. When you apply for naturalization, your case is best supported if you can show some legitimate ties to the country. This includes the ability to speak basic Spanish and demonstrating that you are involved in the local community.

Cost: Living expenses **Time**: 5 Years

Cyprus

A Cyprus passport is less attractive after the financial crisis of 2013. You have two options, both of which require a large amount of money.

- Invest 2,000,000 euros into Cyprus businesses, with at least 500,000 euros of that amount as a donation to the government's Research Fund. If you don't want to make a donation, you must invest 5,000,000 euros.
- Deposit 5,000,000 euros in a Cyprus bank for three years.

Cost: $2M - $5M Investment + $500,000 donation **Time**: Not Applicable

Dominica

This Caribbean country's passport program only offers a donation option. This means your entire "investment" will not be recovered. The most affordable passport program options cost approximately $130,000 for an unmarried applicant.

Cost: $130,000-$150,000 **Time**: Not Applicable

Grenada

Grenada offers a real estate investment option that requires a $500,000 investment. However, that investment must be made in only one government-approved development, and obtaining a second passport in Grenada comes with a residency requirement. You must actually reside there most of the year.

Cost: $500,000 investment **Time**: Not Applicable

Malta

Malta was a great option until their corruption was exposed. An amendment passed in 2013, legally granted eligible persons EU citizenship via Malta by investment in the Malta Individual Investor Program. To be considered eligible for the Malta citizenship scheme, the applicant must be at least 18 years of age and meet several immigration requirements. The Malta citizenship by investment program has some of the strictest due diligence standards of any immigrant investor program in the world. Applicants must have a clean criminal record and must provide a police certificate before they will be approved for European citizenship. All individuals and families applying to the Malta Individual Investor Program must make a significant non-refundable contribution to the National Development and Social Fund set up by the Government of Malta and run by a board of trustees. The following contributions must be made within four months of being issued a Letter of Approval in Principle:

Main applicant - $650,000
Spouse - $25,000
Minor children - $25,000 to $50,000 each
Dependent parents & grandparents - $50,000 each

Applicants must commit to retaining an immovable residence in Malta for a minimum of five years. This can be done by either buying a property in Malta for at least $350,000 and maintaining ownership for five years, or by leasing a property for five years or more with a minimum annual rent of $16,000. Applicants are also required to invest at least $150,000 in government approved financial instruments such as bonds, stocks, and debentures that benefit the nation. Upon purchasing real estate or entering a property lease in Malta, investor citizenship candidates are issued a Malta identity document called an eResidence card. This signifies the commencement of their residency in Malta and also demonstrates the candidate's genuine link with the country. Twelve months after an applicant has established residency in Malta, he or she will be granted citizenship. Maltese law defines residence as "an intention to reside in Malta for any fiscal year, usually evidenced by a stay of a minimum of 183 days or by the purchase/rental of property together with a visit to Malta".

Cost: > $1,000,000 **Time**: Not Applicable

Panama

Panamanian residency is one of the easiest in the world to obtain. After five years of residency, you are eligible to apply for naturalization. A Panamanian passport offers you visa-free travel in 125 countries. This passport is attractive for many because there are exceptionally low requirements for the amount of time you must be present in the country. This makes for an excellent "Time" option, in which you do not technically need to spend time in the country.

A second benefit is the country's territorial tax system, which means that Panamanian residents and companies only have to pay local tax on their Panamanian-sourced income. As long as your income is earned outside of Panama, it is not taxable by Panama.

The easiest residency option is through the Friendly Nations Visa, which applies to nationals of more than 40 countries, including the U.S., Australia, most European countries, Israel, Japan, Hong Kong, South Korea, Singapore, South Africa, and several Latin American countries. Citizens of any of these countries can obtain residency in Panama extremely easily by merely demonstrating "economic activity" in the country. This does not mean that you necessarily need to conduct any business within Panama. Instead, you can satisfy this requirement by registering a Panamanian corporation and making a reasonable deposit at a local bank. Once you submit your residency application, you are free to leave the country and come back a few months later to collect your documents and ID card.

You do not need to physically reside in Panama. Panama's immigration code only requires that the visa be renewed after two years. Aside from that, you do not need to spend any time there. After five years of residency, you are qualified to apply for naturalization. As always, your naturalization case will be much smoother if you have basic knowledge of the Spanish language and you can demonstrate involvement in Panama's business and social life.

Cost: Living expenses **Time**: 5 Years

St. Kitts & Nevis

I first learned about this option when reading the book *Emergency* by Neil Strauss. He documented his efforts to obtain this passport, which was surprisingly easy. Things have changed. The popularity of this program has introduced much stricter rules and inflated fees. This is the longest running second citizenship program in the world and has been in operation since 1984. To get a St. Kitts passport today, you must choose one of two options:

- Make a donation of $250,000 or $300,000, depending on your family size, to the government's Sugar Industry Diversification Fund. This fund was established to help the workers who lost their jobs when the sugar industry became unviable. This is a gift to the country and not an investment.
- Purchase at least $400,000 in "government approved" real estate. These are extremely overpriced and held specifically for wealthy subjects desiring dual citizenship. While you technically own the properties, there is very minimal chance of ever recouping the cost.

Cost: $250,000 - $400,000 **Time**: Not Applicable

Renouncing Citizenship

In 2018, I had a client who insisted on renouncing his U.S. citizenship. I never recommend this, but his political reasons outweighed my concerns for him. He was confident in his decision, and was ready to proceed with or without my assistance. He had recently acquired a secondary citizenship in one of the countries mentioned here. This is not technically required in order to renounce citizenship, but heavily recommended. If you have no other country of citizenship, you would become stateless. It would be very likely that your request to renounce would be rejected.

Once he had his new citizenship in order, he traveled to that location. You should always schedule an appointment with the U.S. embassy or consulate of the location of your secondary citizenship. During the first meeting, diplomatic officials ensure that you are not renouncing your citizenship under duress. You will also need to complete a DS-4079 form (available at eforms.state.gov/Forms/ds4079.pdf). The second appointment requires you to read an oath in which you state your desire to renounce citizenship. Your documents are then sent to the U.S. State Department, which reviews the paperwork and makes a decision on your case within two months. If approved, you will receive your Certificate of Loss of Nationality. After renouncing your citizenship, you no longer pay future U.S. income taxes, and you will not need to report income unless you invest or do business in the U.S. However, you are required to file a final tax return covering the time between January 1 and the day you renounce. If your average annual net income tax in the past five years was $162,000 or more, or if your net worth is more than $2,000,000, you may have to pay an exit tax. The standard fee for renouncing citizenship is currently $2,350. The exit tax can be 30% of your wealth. Again, I never recommend this. Most people who request information about renouncing citizenship eventually decide it is not worth the hassle and risk. Even if you choose to leave the country and live abroad, possessing a U.S. passport is a luxury that many spend years to acquire.

Expatriate

If you believe you need a second citizenship, I encourage you to first consider becoming an expatriate (expat). An expatriate is someone who lives in a different country other than where they are a citizen. In general, expatriates are considered to be people who are residing in their host country *temporarily*, with the ultimate intention of returning home at a later date. However, many expatriates leave their home country and find they can experience a better life abroad. For this reason, many of them never return home, but do not necessarily require a second citizenship. More details, including popular places for expats, can be found at www.expat.com.

Birth Tourism

There is an additional path to citizenship that I have not yet mentioned. Being born within a country that honors the "jus soli" principle, which means "right of the soil" in Latin, can immediately generate dual citizenship. This means that children born in these countries are granted citizenship, regardless of the nationality or immigration status of the parents. In some countries, being born within the borders of the country is enough to automatically be granted citizenship, even if the parents are there as tourists. Countries with unrestricted jus soli laws include the following.

Antigua & Barbuda	Chile	Guyana	Peru
Argentina	Costa Rica	Honduras	Saint Kitts & Nevis
Azerbaijan	Cuba	Jamaica	Saint Lucia
Barbados	Dominica	Lesotho	Saint Vincent
Belize	Ecuador	Mexico	Tanzania
Bolivia	El Salvador	Nicaragua	Trinidad and Tobago
Brazil	Fiji	Pakistan	United States
Canada	Grenada	Panama	Uruguay
Chad	Guatemala	Paraguay	Venezuela

In some other countries, one can only obtain citizenship for the child if certain additional requirements are met, such as that at least one parent is a citizen or permanent resident, or that at least one parent was born in the country themselves. Notable options include the following, and are not usually recommended.

Australia	Dominican	Germany	New Zealand
Chile	Republic	Hong Kong	United Kingdom
Colombia	France	Ireland	

While it is too late for you to choose where you are born, you can make preparations for your child to possess dual citizenship. Some countries, such as Brazil and Panama, allow the parent of a child born on the soil to go through the expedited naturalization process. I will explain more on that in a moment. First, let's consider reasons why one might choose birth tourism as a privacy strategy for a newborn child.

Immediate dual citizenship: Many people strive to obtain dual citizenship for themselves. It can be very costly and can take years to accomplish. With most birth tourism, dual citizenship is immediate for the child. This can be very enticing for parents with an interest in this topic.

Healthcare: Every year, thousands of babies are born in the U.S. to mothers from China. Parents do this to obtain American citizenship for their children. They spend tens of thousands of dollars to hire agencies that help arrange their trips to the U.S. because America's healthcare system is desired. Many people in China do not trust their domestic medical system, which is underfunded and overburdened. Under-the-table payments to doctors in the form of "hongbao" (lucky money) are exchanged as a way to skip long patient queues or ensure patients are treated well. Canada is also experiencing high rates of birth tourism because of this issue.

Education: Many citizens of countries with poor education systems crave a better option for their children. Being born in most Western countries entitles the child to education choices which would never be present in their parents' home countries.

Travel Restrictions: This was previously explained. Parents that desire less restrictive travel for children throughout their lives can use this strategy to bypass visa requirements from their home country.

Child Limits: Some countries, such as China, impose limitations on the number of children allowed per family. While these laws have been relaxed in recent years, they still exist. Births outside of these countries can bypass restrictions. In China, this requires parents to exclude their children from the Chinese national household registration system, which can present other problems. Overall, this strategy is not usually justified.

Parental Citizenship: This is the primary reason for privacy-conscious parents to explore birth tourism. The child born on foreign soil is often referred to as an "anchor baby". Parents intentionally give birth in a specific country in order to possess a child with citizenship in that country. The intention is to use this connection in order to gain their own citizenship. I will focus only on this strategy for the remainder of this chapter, as it is the most applicable to extreme privacy. Let's walk through a typical scenario, which is loosely based on my experiences with two separate clients, both American citizens. I cite Panama as the desired country of secondary citizenship, but you could substitute many of the "jus soli" countries in its place. The following is presented as a checklist of considerations.

- **Decision**: When a person is expecting a child, there is obviously a small window of time to consider if secondary citizenship might be beneficial to the child's future. I urge parents to consider all options, including eliminating this strategy completely.
- **Timing**: Traveling days before a birth due-date is risky. Giving birth on a plane does not accomplish anything. For those considering a foreign birth, I recommend arriving at least a month before the due-date. This gives time to become familiar with the area without a sense of urgency.

- **Birth**: After the child is born, citizenship of the country is immediate. The birth is reported locally and a birth certificate is issued. In this scenario, the child is a citizen of Panama, regardless of the parents' nationalities.
- **Documentation**: Aside from the official birth certificate, a passport can be requested on behalf of the child.
- **"Home" Citizenship**: If the parent(s) are American citizens, the birth should be reported to the U.S. while still abroad. The 2001 Child Citizenship Act (CCA) outlines the requirements with "a child who is under the age of 18, was born outside the U.S., and has at least one U.S. citizen parent automatically acquires U.S. citizenship upon entry into the country as an immigrant".
- **"Home" Documentation**: The parent can request a Certificate of Citizenship and U.S. Passport for the child. The child's parents should contact the nearest U.S. embassy or consulate to apply for a Consular Report of Birth Abroad of a Citizen of the United States of America (CRBA) to document that the child is a U.S. citizen. If the U.S. embassy or consulate determines that the child acquired U.S. citizenship at birth, a consular officer will approve the CRBA application and the Department of State will issue a CRBA, also called a Form FS-240, in the child's name. According to U.S. law, a CRBA is proof of U.S. citizenship and may be used to obtain a U.S. passport and register for school, among other purposes. This should be submitted, authorized, and received while still abroad. If desired, the entire family, including the child with dual citizenship, can safely travel back to the U.S. legally.
- **Parental Application**: The parents can now apply for fast-tracked secondary citizenship. In our example, Panama's President signed a new law allowing foreigners who gave birth to a child in Panama within the last five years to qualify as permanent residents. Many other "jus soli" countries offer this, but the time, expenses, and requirements vary greatly.
- **Basic Requirements**: In Panama, and most other countries, a nationwide criminal police record of both parents must be filed from their home countries national police force. For U.S. citizens this will usually be from the FBI. If one or both parents have lived in Panama without having left the country for a minimum of two years, he or she can obtain the criminal background report from the Panama police (Department of Judicial Investigations "DIJ"). You must also provide an original birth certificate from the Panama Civil Registry. Finally, you must file a letter of responsibility signed by a Panama citizen. This is usually completed by an attorney.
- **Financial Requirements**: Most countries require proof of economic solvency, such as a letter from a Panama bank displaying adequate funds of the applicants. Countries want to ensure you will not further drain their resources for citizens.

- **Costs**: Our scenario with Panama is on the low end of costs. The average expenses per parent include a $1,050 application fee for the immigration department, $150 for the permanent residency carnet (ID card), and up to $2,000 in legal fees. The high end for other desired countries can be over $20,000 per parent.
- **Time**: Obtaining residency in Panama is almost immediate and full citizenship can take up to a year. Other countries can require up to three years for full citizenship for parents of a child born locally.

I hope I did not make this process sound easy. There are always numerous unexpected hiccups when governments move slowly or scrutinize applications. Overall, I do not recommend this privacy strategy for most people. The following explains some complications to consider.

- **Same-Sex Parents**: Many countries do not recognize marriages of same-sex couples, and may exclude residency and citizenship options for anyone who is not biologically connected to the child. I have seen this in the U.S. In one scenario, a couple experienced hurdles after a birth in London. A child was born via surrogate to a male same-sex couple from the U.S. The baby's parents were married and both were U.S. citizens, but the sperm-donating parent was originally born in Britain. Shortly after birth, the U.S. State Department issued a letter informing the couple that their child was not a citizen of the U.S. at birth. The parent with a genetic attachment to the child had not lived long enough in the U.S. as a citizen to pass his citizenship to the child. The other parent, who was a natural born U.S. citizen, could not establish a "blood connection" to the child. According to the principles of "jus soli", the child was an "alien" to the U.S.
- **Government Scrutiny**: Many countries, including the U.S., Canada, U.K, and Australia, are scrutinizing babies born during birth tourism, and proposing laws to prevent it. I do not recommend this tactic as a way to gain citizenship in these countries.
- **Healthcare**: While this was previously mentioned as a benefit for some expectant parents, it can also be an undesired consequence. Some of the countries which allow this do not possess quality healthcare. You may find yourself in a very uncomfortable situation outside the expectations of healthcare in your home country.
- **Stateless Child**: In a worst-case scenario, you may find all of your effort wasted and your child in a "stateless" condition. The country of birth may not recognize the child as a citizen and your home country may not allow entry of this undocumented foreign person. Always do your homework and seek legal help local to the target destination.

Name changes, dual citizenship, secondary residency, and birth tourism are extreme privacy tactics, but required for some targeted clients. I cannot think of a more powerful privacy strategy when trying to avoid America's surveillance than to simply leave. I close with a warning. Secondary citizenships often carry risks. Some countries require mandatory military enlistment for all citizens. Some apply inflated taxes on secondary citizens. A few are always at risk of financial ruin, and any investments could be lost. I try to discourage clients from these methods unless absolutely necessary. The grass is not always greener on the other side. Also, I can speak from experience when I report that secondary citizenship does not bode well for a security clearance renewal.

Chapter Fourteen

Damage Control

If you applied most of the previous privacy strategies toward your life, you should be in good shape, for now. Around every corner is an invasive threat toward your privacy. Data mining companies, marketers, and government entities continue to want your information. It has extreme value in our data-obsessed world. If you want to keep the level of privacy you created, you must put forward effort to maintain it. This chapter presents many considerations for staying private and secure after all of your hard work.

My first advice is to eliminate all potential online privacy threats such as social networks. There is no way to use Facebook, Instagram, Snapchat, and other similar services anonymously. They all possess numerous technologies which attempt to identify you, your location, and your online habits. If you absolutely must use social networks, only use them within your web browser. Never install mobile social network applications on your devices. Viewing Facebook through a web browser gives you some control over which information it can access. Opening the Facebook app provides a deeper level of access to your device's data.

Hardware technologies are also a constant threat. It is becoming much more difficult to purchase various home electronics without jeopardizing your privacy. Consider the following common purchases and associated concerns.

Home Assistants: Amazon Echo and Google Home devices have seen a surge in popularity and adoption. These are the small devices that listen for you to say "Alexa" or "Hey Google" while in your home in order to assist you with daily tasks. Most users of these devices allow them to conduct searches, display videos, or place orders online with only a voice command. I will never allow these devices in my home. A quick search online reveals numerous reports which provide sufficient evidence for my concerns. Amazon admits that numerous employees listen to you through these devices and that they keep the recordings forever. Google is more tight-lipped, but I expect the same.

Smart Doorbells: The Ring doorbell is now owned by Amazon while the Nest option is owned by Google. These have become a trophy of sorts displayed at the front doors of many households. These devices stream video and audio over the internet from your home. If a stranger is at your door while you are at work, you receive a notification and can interact as if you were home. I completely understand the security value of such a device. However, my

privacy concerns outweigh the benefits. These devices are invasive to your neighbors across the street and provide potential hacking attempts since they are connected to the internet.

Televisions: Practically every modern TV available today has embedded Wi-Fi and software which reports usage back to the manufacturer. Some possess front-facing cameras. This is extremely invasive. Most people express little concern for this, as they never connect the TV to their home Wi-Fi, which is encrypted with a password. This is not enough to prevent connection. Some TVs are configured to connect to any open Wi-Fi, such as a neighbor or coffee shop. You could find the wireless adapter and unsolder it from the board, but you would take a high risk of ruining the TV. My preference is to purchase monitors instead of televisions. Since I connect my TV to a media center and amplifier with speakers, a large computer monitor is plenty for my needs. You may pay a slight premium for this, but I find it justified. If you are not convinced, please consider the following.

Samsung is one of the most popular smart TV manufacturers. During Christmas season of 2019, they made a strong marketing push in reference to their "intelligent" TVs which could control home automation; learn to know your interests; and listen for voice activation through mandatory internal microphones (which are always enabled). They also promoted use of internal cameras (which are always enabled and facing the viewer) and the ability to control your TV from any smartphone. I find all of this invasive to our privacy, but their own privacy policy confirms why I will never have one of these devices in my home.

"…the IBA Service will collect information about your TV viewing history (including information about the networks, channels, websites visited and programs viewed on your Samsung Smart TV and the amount of time spent viewing them) and Samsung Smart TV usage information (such as how long and often you use the apps on your Smart TV). We may use automatic content recognition (ACR) and other technologies to capture your TV viewing history. We also may obtain other behavioral and demographic data from trusted third-party data sources…"

The ACR feature referenced in their policy is the ability for Samsung to collect screen captures of your current viewing, transmit them to Samsung networks, and analyze the content. This could include public channels, streaming services, private content played through external media, photographs, home movies, and anything else which may be present on your screen. Yes, even pornography can be copied and transmitted to Samsung. Do you view personal slideshows of family photos on your smart TV? Technically, those can be collected and transmitted back to the manufacturer. Some online privacy enthusiasts have reported that Samsung transmits data through over 200 connections within ten minutes to various subdomains of samsungelectronics.com. Is this legal? Yes, we agree to their terms of service by simply using the product. What can you do?

The first step is to avoid these features when possible. Never connect your TV to any Wi-Fi. If still concerned, create an open Wi-Fi access point and monitor the TV and router log to see if a connection was made to the open network. If you know your TV has no connection to the internet, you are probably fine. Cover any cameras with privacy stickers as mentioned earlier. Navigate through your on-screen controls and disable everything possible. This does not prevent communication attempts, but should lessen the threats substantially.

Lack of connections will also disable desired features such as Netflix and other premium streaming services. I always recommend a separate media server for these options, such as a Roku, Apple TV, or FireTV device. These have their own privacy issues and concerns, but do not send data to your television manufacturer. Each possesses their own version of ACR, but also allow you to disable the option completely. Personally, I prefer a Kodi media server. This option requires a bit of work to set up, but affords more privacy. The details of a Kodi installation exceeds the scope of this book, but online tutorials are abundant.

My policy is to avoid all unnecessary internet-connect devices as possible. My refrigerator does not need to be online. I prefer to control my thermostat with my hand while in my home. Every time you provide internet access to hardware in your home, you now have an additional attack surface. If you do not constantly apply security patches to these devices, you risk immediate exposure once a new vulnerability is published. It is easier to avoid the problem completely by minimizing the number of internet-connected devices. Even if you think you have a low-tech home, it is still vital to scan for vulnerabilities. I conduct two types of audits often within my home and the homes of clients. The first is to discover any connected devices which may be unauthorized. The second is to scan for open Wi-Fi which could unintentionally be used to transmit data from any devices desired to be offline.

Scanning Devices: Since I possess a pfSense firewall as explained previously, it is quite easy to identify the devices on my network. After logging in to pfSense, navigate to "Status" > "DHCP Leases". This screen displays every device on the network which has been issued an IP address from pfSense. This should include any devices connected through your wireless router, as long as you disabled DHCP from that device and rely on pfSense to provide the addresses. If you see anything with an unusual name, investigate.

Scanning Open Wi-Fi: I first reset the network connections on my iPhone (Settings > General > Reset > Reset Network Settings > Confirm). This removes any known Wi-Fi connections. I then analyze any networks without a lock icon in my Wi-Fi connection screen (Settings > Wi-Fi > Networks) while I move around my property. If I locate any open connections which I control, I make the necessary changes. If I find a neighbor with open Wi-Fi, I politely tell them about the risks associated with this behavior. My goal is to simply eliminate any open Wi-Fi which could be used by any device without my authorization.

Kindle and Other E-Readers

You may be surprised to see a section devoted to electronic book readers, such as the Kindle. After all, what could be invasive about reading an e-book? You may be surprised. If you are using a Kindle, Amazon collects and stores the following details about you in your profile, and then shares it with third parties (with your consent from the Terms of Service with which you agreed when activating the unit).

- All books which you have purchased through the device
- All books which you have read through the device
- All books which you have searched from the device
- The last page read of any book in your account
- Any annotations, highlights, or markings within all books
- Speed at which you read any book
- Device language setting
- Wi-Fi and Bluetooth connections
- Estimated locations
- Signal strength
- Times and dates of usage
- Device log files

Some will argue that this is not a big deal. Those people probably did not make it this far into the book. I believe that this is a very big deal. Per the Electronic Frontier Foundation (EFF), this data is shared upon request with law enforcement, civil litigation attorneys, and other Amazon services. If you are involved in a lawsuit, your reading habits, including the date and time that you read a specific chapter, are available to the case. If that happens, this can become public record. Imagine that you are in a child custody dispute or a bitter divorce. If you have been reading books about privacy and security, moving to a foreign country as an expatriate, or growing cannabis, these titles may be used to paint you as shady or unfit. It may be argued that you were reading privacy books to conceal an affair. Your interest in a book about living overseas may be construed as you planning to flee the country to avoid child support obligations. A book about cannabis may be used to make you look like a drug dealer.

Amazon obtains this data when you connect your device to the internet. This happens over the internal Wi-Fi or cellular connection within the unit. The easy solution is to turn off the connection. However, this is also how you obtain new books and have them sent to your device. I encourage you to withdraw from this type of data collection by using the following techniques. I will assume that you are purchasing a new Kindle, but the steps can be applied to existing units. Please note that only a new Kindle will give you complete anonymity. Any existing device already possesses your personal information.

- Purchase a new Kindle from Amazon using a new account created in an alias name. Pay with a masked card for added privacy. Never attach this account to your real name or home address. Ship the device to your CMRA Box or Amazon Locker. Register the device with this account and use any alias name for the Kindle.
- Turn the device on while outside the range of any public Wi-Fi. This could be in your home if your wireless router is secured with a password. Immediately place the Kindle into airplane mode which will disconnect any wireless connections. Never disable airplane mode.
- Order any books for this device from the same Amazon account which was used to purchase the Kindle. The books you purchase will only be accessible on this specific unit. Change the default option of "Deliver to Kindle" to "Transfer via Computer". Your Kindle will be listed on the following screen. Select "Deliver to:"
- A file with the extension of AZW will be downloaded to your computer. Connect your Kindle to your computer via a USB cable. You should see your Kindle listed as a new drive. Copy and paste the book into the Documents folder of the Kindle. Unplug the device and you can now read this book without invasive tactics.

If the Kindle never leaves airplane mode, you will not share any data from the device. Furthermore, the Kindle cannot retrieve new advertisements to place on your home screen. If your device has never touched the internet, there will never be any ads. Amazon will know the books that you have purchased, but will not know who you are. They will not know the details of your reading and annotating. They cannot target you with ads similar to books that you like. If you plan on purchasing a Kindle, I recommend creating a new Amazon account, and using this account only for Kindle-related book purchases.

Sanity Check: We are diving down the rabbit hole of connected devices. We should pause a moment to weigh our risk versus reward. Technology is amazing. The ability to connect our devices to the internet provides wonderful benefit and entertainment. Going too far with disconnections may quickly upset others in your home. Before blindly eliminating internet connectivity from every device you own, consider a conversation with others about the usage and risks.

There might be a middle ground which can gain more privacy while enjoying some of the features of the various devices which you have purchased. I have found that discussing these issues with family before "laying down the law" can create better acceptance of your desires and paranoia. Ultimately, try to involve those who will be impacted by your decisions. While this book is titled *Extreme Privacy*, and my personal application of these tactics are "all or nothing", every situation is unique. Again, pick your battles wisely.

DNA Kits

Consumer DNA testing kits, such as those from 23andMe and Ancestry.com, provide a detailed map of your genealogy which can include information about your family history and potential diseases to which you could be susceptible. These home testing kits usually require a cheek swab or saliva sample which is mailed to the company. That sample includes your unique genetic code. Most companies will share that data with law enforcement, sell it to third parties, and provide it for numerous lucrative research projects. In the future, it could influence insurance premiums or the ability to obtain insurance at all. I find this frightening.

Many of my clients have asked how to utilize these services anonymously. In simple terms, you cannot. You could order a kit using an alias, masked credit card payment, and anonymous mail drop, but that would be the end of your privacy. Since your DNA sample is unique only to you, it would not take long to discover your true identity. Once another family member submitted a sample using their true name, your sample would be associated due to the genetic lineage. After enough samples were collected from other family members, public data could be used to make the connection from them to you. I strongly recommend avoiding these services, and I encourage your family to do the same. If you think I am being paranoid, research the warning issued by the Pentagon in December of 2019. In an internal memo, Pentagon leadership urged military personnel not to take mail-in DNA tests, warning that they create security risks, are unreliable, and could negatively affect service members' careers.

I suspect that most readers of a book such as this would never want to have a third-party company sequence their DNA, so I will stop the sales pitch for avoiding this technology. Instead, let's focus on what can be done if you have already submitted to this type of testing. We know that your data has already been shared, but you can stop future privacy violations. The following instructions will prevent your stored DNA data from being shared or sold by the top three providers.

23andMe: Log in to your 23andMe account and navigate to the account settings page. Click the "Delete Your Data" option under "23andMe Data". Download all of your data before you destroy it. If you agreed to have your physical sample saved, it will be destroyed. Some data, including your DNA, gender, and date of birth, will be retained in order to comply with various medical regulations. However, the company will no longer use or share that information.

Ancestry: Log in to your Ancestry account and click the "DNA" tab. Choose "Your DNA Results Summary" and click "Settings". Choose "Delete Test Results" and re-enter your password. This process will delete your DNA data and prevent you from appearing in any "family finder" results. If desired, you can delete your entire Ancestry account. Your DNA information will be retained for regulatory compliance purposes, but no longer shared or sold.

MyHeritage: Log in to your MyHeritage account and click your name in the upper-right corner. Choose "Account Settings" and scroll to the bottom of the page. Click "Delete Account". Since MyHeritage labs are CLIA-certified, they will still retain some information about you, but no longer share or sell any data.

Removing this data prevents unauthorized breaches from leaking your sensitive details; private companies from profiting from your DNA; and whatever future risks may surface once companies execute new invasive uses for your genetic profile. I believe we are in the infancy of abuses of DNA data.

Fitness Trackers

Digital health monitoring devices have become very popular. Both Google and Apple understand the value of the mass amounts of personal data captured by these gadgets. It would be very easy to simply state that you should avoid all fitness tracking devices, as they all suck up your personal health data for their own benefit. However, I hear from many people who apply these devices to their daily grind in order to obtain better health and a happier life. Therefore, I provide a few considerations for privacy while benefiting from the features.

First, I absolutely avoid anything manufactured by Fitbit. While some of the older devices have the ability to protect your data, anything purchased recently provides user data to the manufacturer. Alphabet Inc., the parent company of Google, announced its intent to acquire Fitbit on November 1, 2019, pending approvals. The sale is expected to close in 2020. This acquisition provides all collected health data to Google for any use desired. I also avoid anything from Apple. While their business model is hardware sales, and they tout privacy as a fundamental right to its users, they are still a huge company which could benefit from the sale of the health data of millions of customers.

This leaves many independent companies which offer various levels of privacy and security within their devices. I suggest looking for devices which provide the following features.

- Allows you to disable Bluetooth and Wi-Fi
- Enables all features without creating an account with the manufacturer
- Allows you to operate the device without internet access
- Provides enough storage capacity to retain collected information within the device
- Does not require connection to a mobile device

As technology capabilities increase, finding a fitness tracker which respects privacy will become more difficult. I encourage you to research older devices instead of the latest trends.

Financial Data Aggregators

I started my first business in 2006. I began using a service called Mint to organize the finances of the company. Mint was later acquired by Intuit (Quicken) and many new features were added. The online service connected to my bank, downloaded all transactions, and helped me understand the flow of my finances. It relied on a service called Yodlee to keep the connection from my bank to Mint alive. At the time, I never considered the privacy implications of using this type of service.

While I allowed my accounts to be updated daily, third parties were allowed to analyze my transactions and sell that information to practically any other company. Today, there are an abundance of financial data aggregators which will happily facilitate connections to your accounts in order to collect data about you. Quicken, Mint, Yodlee, Plaid, Banktivity, and many others generate billions of dollars of revenue thanks to your data. Consider the following example.

Assume you have a software program, such as Banktivity, installed on your computer. You have paid for the annual service which synchronizes the transactions from your bank account to the software. You can now conveniently keep tabs on your money. However, Banktivity relies on synchronization services from Yodlee, which is now owned by Envestnet. Envestnet receives and analyzes all of your transactions and packages that information for sale to the majority of large financial institutions. Every transaction you have ever made is now in the hands of countless banks, investment firms, and credit providers. This happens without a warrant, since you agreed to the sharing by simply using the product. Today, Envestnet has over 3,000 employees and over a trillion dollars in assets under management.

I encourage you to avoid any service which offers to analyze your financial data or connect to your bank accounts. The convenience does not outweigh the privacy violation. The information collected by these companies could be used to influence insurance premiums, credit scores, or loan applications.

As I write this section, the Wall Street Journal reports that Yodlee is accused of selling consumers' personal financial data without proper consent. Three lawmakers submitted a letter calling on the Federal Trade Commission to investigate the matter. Yodlee, now a unit of Envestnet, currently aggregates data from consumers' financial accounts within 15 of the 20 largest U.S. banks, impacting more than 25 million users globally. The letter partially stated "Consumers' credit and debit card transactions can reveal information about their health, sexuality, religion, political views, and many other personal details. Consumers generally have no idea of the risks to their privacy that Envestnet is imposing on them". I suspect we will soon learn of new ways that companies such as this are violating our privacy.

Unintentional Sharing by Friends & Family

Next, consider your future circle of trust. For many clients, their worst privacy exposure is created by their friends and family. Friends may accidentally expose your home address when they post photos to social networks, and family members will not understand why they cannot send Christmas cards to your home address in your name. This is a delicate consideration which should be discussed with everyone in your household. For my clients with extreme privacy needs, I take a very strict stance. The only people in your life who should know your address should be those who will continuously visit you at your home with your consent. Even then, use caution.

I know this sounds restrictive and harsh. The reality is that every weak link in your privacy strategy is one accidental action away from exposing your hard work. Some clients prefer to visit friends and family instead of welcoming them into their own home. Most provide the PMB address as the only mail contact for cards and letters. You must strongly consider the amount of accurate information you are willing to share and with whom. For many years, I knew people who would temporarily hide any number markings on their home when friends visited. This prevented them from writing down the address and later accidentally exposing it. Today, online maps and GPS eliminate the need for a posted address. Your guests' smartphones are a much bigger threat over human error. I cannot tell you how to approach your own family and friends, but I can disclose a few scenarios that have helped my clients.

When my family visits me at my home, I have a strict faraday bag rule. In my case, I meet them at the nearest town and escort them to my property. I blame poor Google Maps directions and my concern they will get lost. When we meet in town, I collect their phones in a large Faraday bag. They know I am a bit eccentric and no longer question many of my antics. I tell them that they will have a means for communication once we get to the home and assure them that a weekend without phones will be great for all of us. At the house, I provide a community laptop which I have never used with my own accounts. It has a Debian Linux operating system and a Firefox browser (with strong privacy settings). The laptop is connected to my guest Wi-Fi protected by my firewall with VPN. They can visit any website, check any email, and enter any passwords they choose. They can stay connected without exposing my home address through cellular towers or GPS data.

I realize that this will not work for many readers. Most people will refuse to give up their phone and must be connected at all times. I respect their decision and offer to spend time with those people outside of my home area. I am also fortunate that there is no active cellular signal on my property. This was very intentional.

Disinformation

Misinformation is when a person unintentionally provides inaccurate information which causes inappropriate content to be released or replicated. I encourage disinformation. This is when a person intentionally provides false or misleading information with an attempt to create inaccurate data. Disinformation is exactly more of what we want to do. Disinformation will help make any accurate data about you seem useless inside a stream of completely inaccurate content.

If you have been extremely successful with eliminating your online information and prohibiting new data from being acquired, you may not need disinformation. However, if you have found a few services that display your private data, or simply want to harden your overall security, disinformation may be the perfect solution. Before proceeding, consider whether this action is right for you. Completing these tasks will add more information about you to the internet. Since the information supplied is false, there is little privacy concern. However, this will lead to much more content available about your name.

Many people like this because it creates a difficult scenario when someone tries to locate them. Some people do not like this tactic because it makes their name more visible throughout the internet. Only you can determine if this action is appropriate. Understand that it may be difficult or impossible to remove the false information which you provide.

This section will identify possibilities that you may consider for your own disinformation attempts. They are divided into three specific groups. The options are endless, and I encourage you to email me any great ideas that you have.

- **Name Disinformation**: This will focus on providing many different names to be associated with your real address and real telephone number to make it difficult to identify the true owner of each. This is beneficial for hiding your real name from people or companies searching for information about your address or number.
- **Address Disinformation**: This will focus on associating various addresses with your real name to make it difficult for people or companies to determine which address is your real home.
- **Telephone Disinformation**: This will associate various telephone numbers with your real name to make it difficult for a person or business to identify a valid number to contact you.

Name Disinformation

Name disinformation will create an appearance that numerous people live at your residence. This could increase the delivery of mail and advertisements to your house. However, none of it will jeopardize your privacy. In fact, it will raise your level of privacy quickly.

Earlier, I explained how to use alias names in connection with your home address. When you activate internet service using a prepaid card, you have the option to use any name desired. The information you provide will eventually be released to third-party data companies. This is a form of disinformation. There are two routes you can take with this. You could choose a different alias name for every bill and service, which will generate chaos. This may be desired, but I prefer a more reserved approach. I choose a single generic name and place various bills under that name. This creates a strong appearance that this person is the true resident. Even if you place your utilities in the name of a trust or LLC, the companies will still want to attach a name to the account. Alias name consistency can create an appearance of legitimacy.

Next, identify a couple of popular magazines for which you are interested in a subscription. Conduct a search for that magazine plus "free subscription". You may be surprised at the abundance of magazines that will give anyone a free subscription. I have found Wired, Forbes, and numerous technology magazines to continuously offer free trials. The most vital part of this exercise is that you do not provide anything close to your real name. Additionally, provide a different name for each subscription. I like to relate each name to the magazine that is being requested. The following could be a guide.

Men's Health: John Sporting
Money Magazine: Tim Cashman
Wired: Alex Techie
Food Magazine: James Cook

I also encourage you not to go overboard. Please only obtain subscriptions that you will read or pass on to someone who will enjoy them. There is no need to waste the product and immediately throw them in the trash. You will also eventually get frustrated if you have several issues arriving every week filling your mailbox.

Similar to magazines, I encourage you to identify a single newspaper that you would enjoy receiving. Newspaper subscriber databases are unique and cater to a specific market. This subscription information will leak out slowly to third-party companies. I do not recommend multiple newspaper subscriptions unless this is appropriate for your daily reading abilities. I enjoy reading the Wall Street Journal every day. A search online for "Wall Street Journal 39 week" will identify dozens of websites which will provide you a 39-week free trial of the paper.

Complete the request and provide a unique name. I have found Mary S. Market to be appropriate. You will begin receiving your print and digital editions within one week.

Trade magazines and mailings are designed to target a specific industry or trade. These are usually free by default and generate revenue from the advertising within the publication. Visiting freetrademagazines.com will display numerous options to consider. I encourage you to be cautious with this method. Many people will load up on magazines of interest and use a false name. While this is acceptable, it does create an association with your home address to your real interests. For example, if you subscribe to seven different web design magazines, and you are a web design artist, this could lead to an accurate profile about the people who live at your home. I would only choose this option if you do not take advantage of a magazine or newspaper subscription.

The time will come when you will need some professional work completed at your home. This will often happen the moment that you stop associating your real name with your home address. Use this as a disinformation opportunity. Consider the following example.

A friend recently discovered that he needed a new roof. Calling a stranger on Craigslist and paying cash would have been acceptable for privacy concerns. However, he understandably wanted to hire a professional company and possess a valid warranty on the new roof. He had recently conducted a complete cleaning of his personal information on the internet, and was concerned that this could jeopardize his privacy.

I recommended that he identify the company that he wished to hire and ask them to provide a quote. He gave them his real address for the roof job, but provided the name of a fake contracting company that was similar to the name of his invisible LLC. If your LLC was named Particle Ventures LLC, you could provide Ventures Contracting. This allowed him to keep his real name away from the process and attach yet another type of disinformation to the address. Upon completion of the work, my friend possessed a written warranty attached to the address and not to a person. This would suffice for replacement if problems with the roof appeared. If you do not possess an invisible LLC, you could use the name of your trust.

Remember, we are not using any of these methods to commit fraud. We are only protecting our privacy and will pay any accounts in full. For most work like this, paying either cash or with a check is acceptable. It is not likely that the name on the check will be attached to the data from the work, but it is possible.

Address Disinformation

This is the most vital type of disinformation if you are trying to disassociate your real name from your real address. The goal with these methods is to create an illusion that you currently live somewhere that you do not. This will make accurate name searches difficult. Before proceeding, you should have an idea of which addresses you will be providing.

This section will explain how to create at least three valid addresses that you will intentionally associate with your real name. The purpose is to show recent activity if someone was to search for you within a people search service. These services always display the most current information first. Therefore, you may want to complete as much of the removal process as possible that is discussed later before providing this disinformation. Additionally, you would only want to do this after you have stopped associating your real name with your real address.

It is very important not to use another individual's home address. While it may not be illegal, it is not ethical and not fair to the other person. If you are hiding from an abusive ex, you do not want to put someone else in danger when he or she decides to break into a house believing it is yours. If you are a police officer trying to protect your family from criminals seeking revenge, you should not send them to some stranger's house and let those residents deal with it. We will only choose locations that do not pose a threat to anyone.

The first address may be a place that does not exist. This is my favorite technique. Many companies possess verification software that will identify invalid addresses. These programs can often be fooled by selecting addresses in new neighborhoods. The following instructions will easily identify a new address for you.

- Conduct a Google search for "new construction city, state". Replace "city, state" with a location at least a few towns away from you. I also recommend clicking "Search Tools", "Any Time", and selecting "Past Year". This will display recent results.
- Choose a search result that connects to a real estate website which displays new homes for sale. The newly planted grass, identical houses, and identical sale price in each listing are also indicators of a brand-new neighborhood.
- Conduct a search on Zillow.com for the highest number visible on the chosen street. You should see a house attached to this address. Increase the address by ten or twenty numbers. In this scenario, I searched 1017 Park Charles Blvd. Zillow informed me that there was no house at this address.
- Search this new address on Google maps and confirm the house does not exist. Switch to the satellite view and confirm there would not likely be enough land to add the number of houses necessary to create this address.
- Document this new address and use it for disinformation.

Occasionally, advanced verification software will identify a fake address as invalid. You may need to provide a real address that is listed as residential but does not belong to an individual family. You may want to choose the address of an emergency shelter. The residents in these are constantly changing, and most of them have 24-hour staff and security. Since many people must consider these a temporary residence, the addresses often defeat the most advanced verification services. Choosing a city and searching it online including the terms "shelter", "men's home", "women's home", and "homeless" will usually provide options. I use this as a last option.

Public library addresses are almost always identified as commercial, but the addresses will pass standard validation. For most disinformation purposes, the address of any public building, including a library, will suffice. Now that you have some ideas for your new address, the next techniques will help you populate online records with this information.

A less invasive way of populating bad information about you on the internet is responding to television offers during infomercials. You have likely seen various offers for information about devices such as medical alerts, home security systems, and reverse mortgages on both daytime and late-night television. They all offer to send you an informational packet describing how they can help you in any situation. These are always a profitable business anticipating huge financial returns when they engage you for their services. Instead, I will use this as a way to mask my true home address.

I recently watched a commercial for a slow motorized device created to help the elderly and those with disabilities. It was a combination of a wheelchair and a moped that could move anyone around the street, grocery store, or mall. You are probably familiar with these "scooters". I called the number and requested information. I used my real name and an address in a new subdivision that did not exist. I do not like to use real addresses because someone will need to deal with the junk mail that is received. This way, the mailings are simply returned to the business. I purposely provided a street name that I located called "Mobility Way".

Within 90 days, while conducting a routine query of my name on people search websites, I located an entry for me on "Mobility Way". I now know with certainty that this company shares personal information. If someone is trying to locate me, he or she will have one more address to research and be disappointed.

There is no need to wait in front of a television all night with the hopes of catching a great disinformation opportunity. The internet has thousands waiting for you at all times. Searching for any of the following topics will likely present numerous websites eager to send you a free information packet. Providing your new "fake" address will get you quickly listed within several marketing databases with this false information.

Home Scooter
Time Share
Home Alarm
Lawn Treatment Service
Home Food Delivery

I have also found that ordering promotional information from vacation, cruise, and retirement related companies quickly shares your personal information. Please do not ever provide any real information about yourself, besides your name, to any of these services. Never provide a credit card number or any other type of payment information. You should only use this technique to create the illusion that you live somewhere other than your real home. Additionally, if you have a common name, such as John Smith, address disinformation is not likely necessary.

Be aware that paper mailings will likely be delivered from, and returned to, the businesses that you contact. This is very wasteful for both the business and the planet. I encourage you to only perform the actions necessary to obtain your address disinformation goal. I do not encourage you to unnecessarily contact hundreds of companies. It only takes a few large companies to make an impact on your overall address identity.

Advanced Address Disinformation

The previous methods will provide a small layer of privacy disinformation. None of those tactics will fool the big players. Ordering marketing materials in your name to a non-existent address will not populate the desired information within premium data mining companies such as CLEAR, Lexis-Nexis, and TLO. These providers only purchase and distribute vetted data, and place emphasis on lines of credit and public records. Some people may want to push bad data to these services, but I urge caution before considering the following techniques.

In 2019, a client insisted on populating address disinformation into the premium data broker providers. He knew that a potential employer would be conducting a background check which included an inquiry into a premium data service. This client lived in an anonymous home with no ties to his true name. He would not consider providing his actual home address to the potential non-government employer. However, this company demanded to possess a "home address" for all employees. Any address provided would be matched to online records from the premium services. He needed an address to provide on the application which would be present within his premium records profile.

This approaches a grey area in terms of legalities. Lying to a private company about your home address is likely not a crime. Creating disinformation about your home address within data mining companies is also likely legal. Generating false data with the intention of fooling a

background check enters new territory for me. If he were applying for a government position, I would have backed away from this request as it could easily cross the line of criminal behavior. Since this was a private organization, I decided to pursue the opportunity.

The first step was to choose an address. This was much more important than using Zillow to find a vacant lot. This needed to be precise, and a place where the world could assume that he lived there indefinitely. We chose a large apartment building near the place of potential employment. For purposes of this example, the address was 1212 State Street. Over 100 apartments were in the building. A quick physical sweep indicated that the apartment numbers followed a pattern of the floor number followed by the room number. The last apartment on the fifth floor was 528. The address for that apartment was 1212 State Street, Apt 528. There were no rooms with 30 in the address on any floor. Therefore, we chose an address of 1212 State Street, Apt 430.

Most address verification systems only consider the street address when associated with apartment buildings. Any apartment number should pass automated scrutiny as long as the street address is correct. My client was confident that the background checks did not include an interview of neighbors or physical inspection of the provided home address. He simply needed an online background check to confirm an address.

Next, we entered an AT&T cellular telephone store and ordered new service. This required a government ID, SSN, and soft-pull on his credit. This violates everything I teach for most clients, but this situation was unique. My client wanted new credit established in order to manipulate the details present in data mining databases. He picked the most inexpensive plan and lowest quality mobile device offered. He would not be using it, and would only abuse the credit inquiry to his benefit. He displayed his DL and provided his real DOB and SSN. He entered the new apartment address on the application and advised that he has recently moved into this new address. The AT&T employee ran the credit check and my client was approved. The system did not care about the mismatch of an address since the applicant was present in-store with a copy of valid identification. Replicating this attempt online would have likely failed.

I chose AT&T intentionally. In my experience, they always require a soft pull for any new line of service. They also provide the full application details, including the home address, to the services which they use for the credit pull. I have found AT&T to release more details to data mining companies faster than other providers. Also, AT&T provides a money-back guarantee. If my client were to return this unused phone within a few days, he is very likely to receive an entire refund. In this scenario, he wanted to keep the number for additional disinformation. The phone would stay in a Faraday bag at all times.

Next, he traveled to a local Best Buy and applied for an in-store credit card. Again, this made me cringe a bit, but I understood his intent. He provided his DL, DOB, SSN, and new apartment alias address. Since he was in-store with proof of ID, he was approved for a card with a low credit limit. He made a small purchase with this new line of credit card paid it off immediately.

Within three weeks, we saw evidence of this new address on both his credit report and premium data report. While any investigator would see right through this, it was enough to pass the scrutiny of a standard background check using premium records. He then applied for, and received, his desired job.

For the record, I do NOT recommend these actions for the vast majority of my clients. It is usually unnecessary and can present additional problems. Any future background checks may need to explain this discrepancy on a public report. A government clearance may be denied when you disclose your antics of attempted disinformation with an alias address. There are many more reasons NOT to apply this technique than valid scenarios. I present this only as a tactic to possess in your arsenal of tools.

Social Networks

I usually do not promote the creation of personal social network profiles. However, they can be very useful in some cases. I once consulted a young woman who was the victim of severe harassment by a man who was a former high school classmate of hers. His unwelcome approaches caused her to move and purchase a different vehicle. She was doing well at staying off his radar, but still knew he was looking for her. She created a Facebook page, added a couple of photos of her pet, and publicly displayed her location as a town over an hour away. While monitoring the Twitter account of her stalker, she observed him "check into" a bar in that very town, likely looking for her. While this does not solve the issue long-term, it provided enough uncertainty to confuse the stalker and waste his time.

Creating several social network profiles and including publicly visible location data can be beneficial. You can either make them very confusing by placing different locations on each profile, or place the same city on all of them to create a convincing situation. For most clients, I find LinkedIn to offer a great platform for disinformation. I can create an account, provide a real name, and choose any current workplace and location desired. This can quickly throw an adversary off my client's trail if he is actively trying to locate him or her. Aside from LinkedIn, I find Instagram, Twitter, Facebook, and TikTok accounts valuable for online disinformation. However, always apply the digital security principles discussed earlier. After the accounts are created, never log in to them unnecessarily and always use a VPN.

Telephone Disinformation

Receiving unwanted telephone calls from telemarketers can be annoying. Calls from them to random numbers are unavoidable. However, targeted calls specific to you can be extra frustrating. You have already learned how to eliminate public record of your telephone number. You may now want to populate disinformation to prevent a person or business from discovering your true home or cellular telephone number.

Before you can provide the false telephone number information with hopes of it being attached to your name within public databases, you must select some appropriate numbers. Most importantly, you never want to provide a false number that belongs to another individual. That is not only rude, but it can also jeopardize that person's right to privacy from unwanted callers. Instead, focus on telephone numbers that either do not exist or belong to services that are never answered by an individual.

My favorite telephone numbers for disinformation are numbers that are always busy and cannot be answered. These were once abundant, but many of them have now been assigned to customers. There are still two large groups of telephone numbers that will always be busy when dialed. The following sets of numbers should work well.

909-661-0001 through 909-661-0090
619-364-0003 through 619-364-0090

The 909 area code serves the Los Angeles area of California and the 619 area code serves the San Diego area. These were early line numbers when service began in these areas and the numbers should not be assigned to any customers. Since these are not toll-free numbers, they should not be flagged as non-residential. Because numbers are ported so often, possessing a number in another area code should not raise any suspicion. When you give someone a number that is always busy, it does not create the appearance of a fake number. These may appear real to a person that would otherwise question the validity of a given number.

There are plenty of unused numbers that announce "disconnected" when dialed. Most of these are temporary and will be assigned to a customer at some point. The following range of numbers all announce a "non-working number" when dialed. The area code serves Pennsylvania. Giving one of these numbers to a person or business can enforce a desire to not be contacted. Always test the numbers which you choose before using them.

717-980-0000 through 717-980-9999

One of the quickest ways to associate a false telephone number with your real name is to enter various contests. You have probably seen a brand-new vehicle parked inside your local

shopping mall. A box next to it likely contained blank pieces of paper asking for your name, address, and telephone number with promises that someone would win the vehicle. Have you ever known anyone that won a vehicle this way? I do not. Instead, these gimmicks are often used to obtain a great list of potential customers that might be interested in automobiles. This content is often combined with other contest data and sold to numerous companies. Eventually, the provided information is attached to you through a marketing profile that may follow you forever.

In years past, I have always laughed at the idea of entering these contests. Today, I never pass up this opportunity. I always provide my real name, my false address from the address disinformation section mentioned earlier, and one of the "busy" telephone numbers previously listed. I like to use different numbers every time and watch for any online associations to me from these numbers. I then know which contest companies are selling my information.

Most grocery stores have a shopper's card program which provides discounts on merchandise. These are portrayed as opportunities to save money for being a loyal customer to the brand. In reality, these cards are closely monitored to learn about your shopping habits. This data is used to create custom advertising and offers. The only benefit of joining this program is the savings on the items which you purchase. The risk of joining is the guaranteed profile that will be created about you and sold to interested parties. However, you can enjoy the benefits without jeopardizing your privacy. This is a great opportunity for telephone disinformation.

Practically all of the stores which utilize this type of savings program allow you to access your account by the telephone number that you provided during registration. You are not required to provide or scan your shopper's card. You can simply enter your telephone number to obtain the savings and attach your purchases to your profile. I have found the telephone number of 867-5309 to work at most stores. This number may not look familiar, but say the number out loud. This was the title of a song by Tommy Tutone in 1982 that gained a lot of popularity. This number is currently assigned to customers in most area codes. In fact, it is often sought after by businesses due to the familiarity. I never use this number with services that may try to contact me. Instead, I only use it when I register a shopping card at a grocery store.

If I am shopping in Chicago, I use an appropriate area code, such as 847. If you ever find yourself at a Safeway store anywhere in the world, you can use 847-867-5309 as your shopper's card number and it will be accepted without hesitation. If you find that this number does not work at another chain, you should consider requesting a shopper's card and provide it as your number. I provided my real name, the disinformation address discussed earlier (which does not exist), a Chicago area code, the 867-5309 number, and a specific email address at my 33 Mail account. I will never use that email account again, and will know which company

provided my information when I receive unwanted email at Safeway@nsa.33mail.com. I can now provide 847-867-5309 as my member number when I shop at Safeway. You can too.

As a community service, I create new accounts at every store that I can using the number of 847-867-5309. The more strangers that use this number during their shopping, the more anonymous we all are. The data collected by the store will not be about one individual. Instead, it will be a collective of numerous families. If you locate a store without a membership with this number, please consider activating your own card with address disinformation. Within weeks, this information will be associated with your real name. It will add an additional layer of anonymity by making any present information difficult to find and harder to prove accurate.

Business and 411 Disinformation

Regardless of whether you desire name, address, or telephone disinformation, you should consider business listings. Most of these types of websites allow a personal name to be used instead of a business name. Any data provided will replicate all over the internet quickly. The first service which I submit is listyourself.net, followed by Google Maps and Yelp. The irony of suggesting these free services is that most of my clients want to avoid them or remove their information. Any data provided here, such as your name and address, will be populated across multiple people search websites within weeks. However, we can use this as a strong disinformation strategy. Before conducting any of the following tasks, consider your goals and what types of disinformation you want to be publicly available. You cannot change your mind later on this one. Whatever you give them is permanently public data. Consider the following steps I took on behalf of a client.

This client had successfully moved into an anonymous home, but knew her abusive ex-boyfriend had been released from jail and was actively pursuing her new location. A disinformation campaign was appropriate in her scenario. I visited listyourself.net and chose "Individual, personal or business listings". I then provided the following details for each field.

- Phone number: I chose a telephone number of the hotel where I was staying at the time, in a city far from the client's home.
- Name: I provided my client's real name.
- Country: I entered my client's true country.
- Address: I supplied an address of a large apartment building in a city far from the client's home. New York City has many buildings with over 500 units each. This is the address I will publicly associate with my client, without an apartment number.
- Email: A ProtonMail alias address used for "junk" in the name of the client. This address is not associated with any online accounts or login portals.
- Validation Method: I chose the "Call me with a spoken code" option.

This service will waive any fees as long as they can confirm you have provided a true telephone number. Before I clicked "Add Listing", I took my laptop to the front desk of the hotel and spoke to the front desk clerk. I told her I was trying to connect to a web call with my boss, but it wants to verify my location. I asked "Can I have them call your main line and have them give me a code?", which she happily allowed. The telephone rang, she answered, and repeated the automated code she was given during the call. My listing was approved. Next, I navigated to www.google.com/business and signed in with an alias Google account which I only use for this purpose. I then conducted the following steps.

- Enter the name of my client as the business name
- Confirm I wish to add a location
- Enter the address used previously, and click Next
- Confirm that customers are not served outside this location
- Provide a generic category such as Personal Trainer
- Leave the contact details blank
- Click Finish
- Choose the options to Verify by Phone, and provide the same hotel number
- Repeat the process with the front desk, entering the code provided

Some people have reported that they do not receive the option to verify by phone, and can only verify with a mailed postcard. I suspect this is due to the Google account being used. My account may have been allowed because it has been active for many years and has activated numerous businesses. If you do not receive the option to verify by phone, do not request a postcard and move on.

Next, I navigated to biz.yelp.com/signup_business/new/ and registered my client for her own personal Yelp page. I provided the same real name, alias apartment building address in the city used previously, junk email address, and a Google Voice number reserved for disinformation purposes. I was immediately sent an email to verify the account, and was forwarded to a page to create a Yelp account for the client. I completed the registration and was asked to verify the telephone number via confirmation code. The Yelp account was then active.

Within a few days, searching my client's name on Google revealed a Yelp page identifying her home trainer business being located in a large apartment building in New York. Google Maps eventually confirmed this address for her home-based business. Her name, alias address, and number were populated on numerous 411-style websites within two weeks. That should keep the abusive ex-boyfriend busy for a while.

Death Disinformation

I hesitate writing this. However, I once had a client who needed to "die" digitally. She had no immediate family, a few close friends, and a dedicated former lover trying to harm her at any chance he could find. During an initial consultation, she stated "I wish he thought I was dead". I cautiously discussed the possibility, which she immediately demanded to be executed. The most bang-for-your-buck option is an obituary in the Legacy network of newspapers.

You can navigate to legacy.com > Obituaries > Submit an Obituary > Select a state > Select a newspaper. You will need to submit the obituary directly to the local paper of choice, and anything printed will be acquired by legacy.com and distributed. Expect a small fee. This will make an obituary extremely public, which can never be reversed. The obituary on legacy.com can be shared on social networks, and really "sells" the death.

Use caution, because some newspapers demand a death certificate. I have found extremely small newspapers near the town of birth of the target are less likely to demand this versus large city newspapers. For extra credit, consider submitting a memorial and photo to Find A Grave at findagrave.com. If your Photoshop skills are not sufficient, contact an online tombstone maker and ask for an example of how your deceased relative's details would look (providing your information). They will create a realistic image and submit it to you for approval.

Overall, I never recommend this strategy. If you are in a situation regarding this extreme activity, contact me first. This could have a severe impact on future credit, employment, relationships, and sanity. If you conduct any level of research into faking your own death, you will mostly find stories of people who were caught doing this. For more information, read *Playing Dead* by Elizabeth Greenwood. I never encourage anyone to commit full pseudocide (faking your own death). Traditionally, this is done to collect life insurance funds, evade outstanding arrest warrants, get out of paying various loans, or simply start over with a new identity. Unless you plan on living in the mountains without any source of income, it simply will not work. Although no federal or state statutes explicitly ban pseudocide, you are likely to commit crimes such as conspiracy or fraud during the process.

My colleague "Mike A." offers one last piece of advice. If you receive undesired mail, such as advertisements, in your real name at your home, and you have asked to be removed from the mailing list, consider a death announcement. He purchased a rubber stamp from a local office supply store which prints "Return to Sender - Addressee Deceased" in red ink on any unsolicited mail he receives in his name. He then drops the envelopes in a nearby mailbox for return to the sender. This seems to have a better outcome than a polite request to be removed. I am ashamed I did not think of this. Please note this will likely only work with first class mail, as the post office does not return flyers and other bulk mail.

Disinformation Concerns

Several government employees have expressed concern to me about the risks of removing all personal information from the internet. Their thinking is that if there is no information about you it could be a red flag that you are affiliated with the intelligence and/or special operations communities and could cause you to come under suspicion in a foreign country. This creates quite a conundrum.

If members leave all their personal information on the internet, their spouses and children could be exposed and placed in danger. This is becoming even more important as we are starting to see targeted terrorism and doxing of military personnel within the borders of the United States. Alternatively, doing so may compromise their status by giving them a digitally "different" profile. I agree entirely with this logic. However, I disagree with the suggestions I have heard for solving this problem. Most of these suggestions are to essentially do nothing and take a more passive posture on social media. This is not my approach.

My solution is to remove all real information to the maximum extent. I believe you should make your home, your vehicles, your children, and your spouse as difficult to identify as possible. Only then will you be able to sleep soundly at night, secure in the knowledge that you and your family are a very difficult target to locate. However, I do not believe you should stop there. My opinion is that disinformation in this case is as good as real information. If the person reviewing it is overseas and finds five separate records of your "home" online, the scrutiny will likely end there.

I am also not opposed to creating social media disinformation. A social media account that is in your true name, but contains no accurate information, will make you look real while preventing you from being compromised. I do not recommend you associate yourself with a social media account under a different name, especially if the account has photos of you. This will almost certainly have the effect of making you look even more suspicious. The more thorough your disinformation campaign is, the more protection it will afford you.

In some agencies or departments, you may be prohibited from doing this yourself. You should check your department, agency, or headquarters policy before undertaking this. Another concern that has been expressed to me is that if you need this level of protection the individual's organization will "take care of it". While this may be the case in some instances, I encourage you to take responsibility for your own security and safety where permissible.

Monitoring

Now that you possess an invisible home with disinformation attached to it, you should continuously monitor your progress. Searching for yourself and your family within various people search websites will confirm your success at staying invisible. This should be conducted monthly until you are confident that any new online data would be inaccurate. Your success at remaining invisible to the growing number of personal data collection organizations will be reliant on your constant monitoring for any new leaks of your details on the internet. I would like to add one technique that I have found valuable for those desiring an aggressive approach toward monitoring situations where other people may be searching for details about them. **Canary Tokens** (canarytokens.org) offers an advanced way to monitor this behavior.

This free service allows you to create a Microsoft Word document, among other options, including PDF files, which includes a tracking script within. Anyone who opens the document will unknowingly launch the script which will collect the user's IP address, approximate location, operating system, and browser information. While an adversary could easily block this type of collection with a tracking script within a website or email, it is more difficult to stop within a document. Consider the following example.

I created a Canary Token document with a title of Michael Bazzell's Home Address and uploaded it to a public document storage site. When a person conducts a search for my name and sees this file, he or she is likely to open it, hoping to finally have my home details. The document is blank, but I am immediately sent the following information.

Date: 2019 Mar 15 16:34:25
IP: 193.0.108.42
Country: US
City: Marietta
Region Georgia
Organization: Comcast Cable

Language: en-US
Platform: MacIntel
Version: 74.0.3729.131
OS: Macintosh
Browser: Chrome

You now have knowledge that someone may be searching for you. These details are the exact data obtained from someone opening the "bait" document. This information tells me that someone was likely researching me from Marietta, GA, on a Mac running Chrome. The IP address confirms they use Comcast as their ISP. I do not know their identity or exact address, but this reveals a potential threat.

Doxing Attempts

Many of these methods may seem ridiculous and inappropriate. If no one ever tries to find you, none of this is necessary. Many of my clients are targeted often, and I like to have false trails leading to inaccurate data. I have also found this to be beneficial for myself. In October of 2018, I was on the receiving end of a full doxing attack.

Doxing is the attempt to search for and publish private or identifying information about a particular individual on the internet, typically with malicious intent. Someone had posted information about a group called 4Chan/8Chan on my online forum. This group is known for hateful posts, doxing, e-swatting, and other malicious activities. Word had spread to the 4Chan/8Chan community that my site was talking about them in a negative way. They decided to attack me as the owner of the site.

Multiple people scoured the internet for any personal information about me. They believed they were successful, but did not uncover anything valid. The cell number they located was a Google Voice account provided on a Facebook page which I have never used. The home address they located was a non-existent house in my former city of residence. The email addresses they found were all intentional burner accounts which did not reach my true inboxes. They were effective in their search, but the data was simply inaccurate. I never predicted a doxing attempt toward me, but I was glad I had taken the necessary precautions ahead of the attack. You can hear more about this incident on my podcast (Episode 096-Lessons Learned from My Latest Doxing Attack).

This seems like an appropriate time to remind readers that we never know when we will be a victim of an online attack. In 2017, two online gamers engaged in a feud over a $1.50 bet. This resulted in a swatting attempt toward one of the players. Tyler Barriss called the Wichita police from his Los Angeles home falsely reporting a shooting and kidnapping at the Wichita address of the other gamer. Police surrounded the home and Andrew Finch emerged from the front door confused about the commotion. After raising his hands at the order of police, he lowered one hand toward his waist. An officer shot him, killing him immediately. Tyler Barriss had conducted dozens of similar calls prior to this in order to harass other online gamers. This incident resulted in a 20-year prison sentence.

It does not take much today to upset someone to the point of taking malicious action against you. The internet has made it easier than ever to locate someone's home address within seconds. Being proactive by creating a safe and anonymous home is the first step toward preventing online attacks. Disinformation provides another strong layer of protection.

Contact Information Abuse

Everywhere we turn, there are attempts to collect our data. Companies want your phone number and email address in order to bombard you with marketing. The data collected becomes stored in company databases which are later sold, traded, leaked, or breached. The aftermath becomes our problem. Because of this, I am cautious to ever use personal communication accounts and rely heavily on forwarding services which were explained earlier. However, there will always be unintentional exposure. Consider the following scenarios I witnessed over the past year.

Appointment Check-in Systems: In 2019, I scheduled an appointment to see a chiropractor before a long business trip. I was notified that they rely on a digital check-in system which now requires me to provide a valid email address or cellular telephone number through a series of iPads on the counter. I had never provided any contact details to this service, so I was not sure what to provide. The staff was very helpful and instructed me to use my first name then @123.com. Apparently, many of these systems accept any email address which ends with @123.com. I recorded one interaction of this for an introduction to my podcast (episode 143). If I had provided a real email address or number, I suspect it would have been abused.

Lodging Requirements: In 2019, I checked into a resort where I was presenting a cyber keynote the following day. My room was prepaid by the conference and attached to the master bill. However, the clerk demanded I provide a valid cellular telephone number and email address. I respectfully declined and she informed me that she could not complete the check-in process without this information. I supplied a random number which was accepted. However, she stated that my email address would need to be verified via a response to a message before she could issue access to my room. She stated that the email address would only be used to contact me in the case of an emergency. I politely advised that I could be contacted at my room if there was an emergency. She did not budge. I provided a 33Mail account which was rejected by the system. Apparently masking services were blacklisted. I reluctantly provided a ProtonMail alias, which was accepted. I told her that I would be forwarding any spam to her if the contact details were abused, and collected her business card from the counter. Within 24 hours, I began to receive marketing emails from the resort. I quickly created a rule which forwarded any messages received from the resort to the clerk's email address. I suspect she was not amused.

This is a tactic which I have used often when a company will not remove me from a mailing list. If I start to receive unwanted and unauthorized spam from a business, I identify the email addresses of any executives. I then create an email rule which forwards to them all messages which I receive from that company, then immediately sends them to the trash. In my experience, my email address is quickly removed from their list once an executive complains about the emails coming from me.

Personal Data Removal

In the unfortunate scenario where you locate accurate personal information on a website, such as your name and home address, don't panic. I maintain a large workbook of data removal (opt-out) options on my website at **https://inteltechniques.com/data/workbook.pdf**. This presents hundreds of invasive websites and the options for requesting removal of exposing information. The removal process of your information is usually easy, with a few exceptions. Most services will offer you a website to request they remove your details. These direct links are often hidden within fine print or rarely visited pages. My goal in this workbook is to take the research out of the removal process and simply tell you where to start. Each removal summary will display several pieces of information about each service that I have identified. The following structure outlines the data that is displayed throughout the next several pages.

Service: The name of the service
Website: The website of the service
Removal Link: The direct link for online removal, if available
Email Address: Any email addresses that will reach an employee responsible for removal
Notes: Any special instructions

All resources are listed in alphabetical order for easy reference. The data supplied in the email address field could be used for unsuccessful removal attempts. If the official removal process for that service does not meet your needs, I recommend sending an email to the company. I have tried to locate email addresses of employees that appear to be responsible for removal requests. I suggest the following message be sent from the anonymous email address that you created earlier.

I have been unsuccessful in removing my personal information from your website. Per the information provided from your legal privacy policy, please remove the following details from your service.

Full Name (As appears on their service)
Physical Address (As appears on their service)
Telephone Number (ONLY if it appears on their service)
Email Address (ONLY if it appears on their service)

I have found the "Most bang for your buck" removals to be Spokeo, Mylife, Radaris, Whitepages, Intelius, BeenVerified, Acxiom, Infotracer, Lexis Nexis, and TruePeopleSearch. Removal from these services will trickle down to many of the smaller sites mentioned on the following pages. I recommend that people start with these first, wait about one week, and then start to tackle the remaining sites. If they ask for a photo ID, just upload something random from thispersondoesnotexist.com. They usually don't even look at the picture.

The following removal options were accurate as of May 2020. These are mostly targeted toward U.S. persons, but a few sites possess data internationally.

Service: 411
Website: 411.com
Removal Link: None
Contact: support@whitepages.com
Notes: Remove entry from whitepages.com

Service: 411 Info
Website: 411.info
Removal Link: 411.info/manage/
Contact: support@411.info, admin@411.info
Notes: Online removal tool will complete the process.

Service: Acxiom
Website: www.acxiom.com
Removal Link: https://isapps.acxiom.com/optout/optout.aspx
Contact: consumeradvo@acxiom.com
Notes: Online removal tool will complete the process.

Service: Addresses
Website: addresses.com
Removal Link: addresses.com/optout.php
Contact: support@addresses.com, admin@addresses.com
Notes: Online removal tool will complete the process.

Service: Address Search
Website: addresssearch.com
Removal Link: addresssearch.com/remove-info.php
Contact: support@addresssearch.com
Notes: Online removal tool will complete the process.

Service: Advanced Background Checks
Website: advancedbackgroundchecks.com
Removal Link: https://www.advancedbackgroundchecks.com/removal
Contact: Unknown
Notes: Online removal tool will complete the process.

Service: Advanced People Search
Website: https://www.advanced-people-search.com/
Removal Link: https://www.advanced-people-search.com/static/view/optout/
Contact: https://www.advanced-people-search.com/static/view/contact/
Notes: Online removal tool will complete the process.

Service: All Area Codes
Website: https://www.allareacodes.com/
Removal Link: https://www.allareacodes.com/remove_name.htm
Contact: https://www.allareacodes.com/contact_us.htm
Notes: Online removal tool will complete the process.

Service: All People
Website: https://allpeople.com/
Removal Link: Embedded
Contact: webmaster@allpeople.com
Notes: Select profile and choose "Remove Listing".

Service: Anywho
Website: anywho.com
Removal Link: None
Contact: ypcsupport@yp.com, press@yp.com
Notes: Select profile and choose "Remove Listing".

Service: Ancestry
Website: ancestry.com
Removal Link: None
Contact: support@ancestry.com, customersolutions@ancestry.com
Notes: Send message to both email addresses requesting specific information removal.

Service: Archives
Website: archives.com
Removal Link: archives.com/optout
Contact: privacy@archives.com
Notes: Online removal tool will complete the process.

Service: Background Alert
Website: https://www.backgroundalert.com
Removal Link: https://www.backgroundalert.com/optout/
Contact: customerservice@backgroundalert.com
Notes: Online removal tool will complete the process.

Service: Background Check
Website: https://backgroundcheck.run/
Removal Link: Within result
Contact: https://backgroundcheck.run/pg/contact
Notes: Online removal tool will complete the process. Lookup name and select "Control this profile".

Service: Been Verified
Website: www.beenverified.com
Removal Link: www.beenverified.com/faq/opt-out/
Contact: privacy@beenverified.com
Notes: Online removal tool will complete the process.

Service: BlockShopper
Website: blockshopper.com
Removal Link: None
Contact: scarlett@blockshopper.com
Notes: Send email with removal request.

Service: Buzzfile
Website: buzzfile.com
Removal Link: http://www.buzzfile.com/Company/Remove
Contact: info@buzzfile.com
Notes: Online removal tool will complete the process.

Service: Caller Smart
Website: https://www.callersmart.com
Removal Link: https://www.callersmart.com/opt-out
Contact: https://www.callersmart.com/contact
Notes: Email submission bypasses account creation requirement.

Service: Cars Owners
Website: https://carsowners.net
Removal Link: None
Contact: https://carsowners.net/feedback
Notes: Email through the website requesting removal.

Service: Catalog Choice
Website: catalogchoice.org
Removal Link: None
Contact: support@catalogchoice.org
Notes: Online removal tool will complete the process.

Service: Check People
Website: https://www.checkpeople.com
Removal Link: https://www.checkpeople.com/opt-out
Contact: support@checkpeople.com
Notes: Online removal tool will complete the process.

Service: Check Them
Website: https://www.checkthem.com
Removal Link: https://www.checkthem.com/optout/
Contact: support@checkthem.com
Notes: Online removal tool will complete the process.

Service: City-Data
Website: https://www.city-data.com
Removal Link: https://www.advameg.com
Contact: others@city-data.com, legal@city-data.com
Notes: Go to www.advameg.com and submit an opt-out request.

Service: Clustr Maps
Website: https://clustrmaps.com/p/
Removal Link: https://clustrmaps.com/bl/opt-out
Contact: https://clustrmaps.com/bl/contacts
Notes: Online removal tool will complete the process.

Service: Complete Investigation Services
Website: www.cisnationwide.com
Removal Link: cisnationwide.com/optout.html
Contact: support@cisnationwide.com
Notes: Fax required documents to 888-446-1229.

Service: Confidential Phone Lookup
Website: https://www.confidentialphonelookup.com
Removal Link: Highlight entry and click "Do Not Display"
Contact: https://www.confidentialphonelookup.com/contact/
Notes: Online removal tool will complete the process.

Service: Contact Out
Website: https:// contactout.com
Removal Link: None
Contact: support@contactout.com
Notes: Send email with removal request.

Service: Core Logic
Website: www.corelogic.com
Removal Link: None
Contact: privacy@ebureau.com
Notes: Online removal tool will complete the process.

Service: Cyber Background Checks
Website: https://www.cyberbackgroundchecks.com
Removal Link: None
Contact: https://www.cyberbackgroundchecks.com/contact
Notes: Send email with removal request.

Service: DataChk
Website: www.datacheckinc.com
Removal Link: None
Contact: https://www.datacheckinc.com/contact.php
Notes: Send email with removal request. Removes data from several subsidiaries.

Service: Data-Records
Website: https://data-records.com/
Removal Link: https://federal-data.com/control/profile?url=
Contact: https://federal-data.com/page/contact
Notes: Paste your original url from data-records.com following the = sign in the removal link.

Service: DirectMail
Website: https://directmail.com
Removal Link: https://www.directmail.com/mail_preference/
Contact: donotmaillist@directmail.com
Notes: Online removal tool will complete the process.

Service: DMA Choice
Website: dmachoice.org
Removal Link: www.ims-dm.com/cgi/dncc.php
Contact: ethics@the-dma.org
Notes: Follow instructions on removal link.

Service: DOB Search
Website: www.dobsearch.com
Removal Link: Embedded into results
Contact: support@dobsearch.com
Notes: Search your name and click "Manage my listings" at bottom. Follow instructions.

Service: Email Finder
Website: https://emailfinder.com
Removal Link: https://www.beenverified.com/app/optout/search
Contact: support@emailfinder.com
Notes: Online removal tool will complete the process.

Service: Epsilon-Main
Website: epsilon.com
Removal Link: None
Contact: optout@epsilon.com
Notes: Send email with "Removal" as the subject. Include name and address.

Service: Epsilon-Abacus
Website: epsilon.com
Removal Link: None
Contact: abacusoptout@epsilon.com
Notes: Send email with "Removal" as the subject. Include name and address.

Service: Epsilon-CFD
Website: epsilon.com
Removal Link: None
Contact: dataoptout1@epsilon.com
Notes: Send email with "Removal" as the subject. Include name and address.

Service: Epsilon-Shopper
Website: epsilon.com
Removal Link: None
Contact: contactus@shoppers-voice.com
Notes: Send email with "Removal" as the subject. Include name and address.

Service: Fama
Website: https://fama.io/
Removal Link: None
Contact: privacy@fama.io
Notes: Send email with removal request.

Service: FamilySearch
Website: www.familysearch.org
Removal Link: None
Contact: RochaJL@familysearch.org, DataPrivacyOfficer@ldschurch.org
Notes: Send email with removal request.

Service: Family Tree Now
Website: familytreenow.com
Removal Link: www.familytreenow.com/optout
Contact: www.familytreenow.com/contact
Notes: Online removal tool will complete the process.

Service: Fast People Search
Website: https://fastpeoplesearch.com
Removal Link: https://www.fastpeoplesearch.com/removal
Contact: https://www.fastpeoplesearch.com/contact
Notes: Online removal tool will complete the process.

Service: Fax VIN
Website: https://www.faxvin.com
Removal Link: None
Contact: https://www.faxvin.com/company/contact
Notes: Email through website to request removal.

Service: Find Local People
Website: https://www.findlocalpeople.com
Removal Link: https://www.findlocalpeople.com/people-locator/change-listing.html
Contact: https://www.findlocalpeople.com/people-locator/contact-us.html
Notes: Online removal tool will complete the process.

Service: Find People Search
Website: findpeoplesearch.com
Removal Link: findpeoplesearch.com/customerservice/
Contact: support@ findpeoplesearch.com
Notes: Online removal tool will complete the process.

Service: Free Background Checks
Website: freebackgroundcheck.us
Removal Link: None
Contact: info@peepdb.com
Notes: Fax submission based on instruction listed on Privacy Policy page to 617-933-9946.

Service: Free Phone Search
Website: https://www.phonesearchfree.com
Removal Link: https://www.phonesearchfree.com/opt-out
Contact: customercare@PhoneSearchFree.com
Notes: Online removal tool will complete the process.

Service: Free Phone Tracer
Website: https://www.freephonetracer.com/
Removal Link: https://www.beenverified.com/app/optout/search
Contact: privacy@ freephonetracer.com
Notes: Online removal tool will complete the process.

Service: Free Public Profile
Website: https://www.freepublicprofile.com/
Removal Link: https://www.freepublicprofile.com/Removal
Contact: https://people.vidalud.com/Contact
Notes: Online removal tool will complete the process.

Service: Full Name Directory
Website: www.fullnamedirectory.com
Removal Link: https://www.dobsearch.com/remove
Contact: support@dobsearch.com
Notes: Online removal tool will complete the process.

Service: GoLookup
Website: golookup.com/
Removal Link: golookup.com/support/optout
Contact: support@golookup.com
Notes: Online removal tool will complete the process.

Service: Haines & Company
Website: https://www.haines.com
Removal Link: None
Contact: criscros@haines.com, info@haines.com, custserv@haines.com
Notes: Send email with name and address and request to be removed from all databases.

Service: Hauziz
Website: https://hauziz.com
Removal Link: None
Contact: support@hauziz.com
Notes: Follow instructions outlined in section one of privacy policy.

Service: HPCC-USA
Website: https://www.hpcc-usa.org/
Removal Link: https://www.hpcc-usa.org/research/change-listing.html
Contact: https://www.hpcc-usa.org/research/contact-us.html
Notes: Online removal tool will complete the process.

Service: ID True
Website: https://www.idtrue.com
Removal Link: https://www.idtrue.com/optout/
Contact: support@idtrue.com
Notes: Online removal tool will complete the process.

Service: Infogroup
Website: infogroup.com
Removal Link: None
Contact: contentfeedback@infogroup.com
Notes: Send email with "Opt-Out" as the subject. Include name and address.

Service: Infopay
Website: https://www.infopay.com/
Removal Link: https://www.infopay.com/new/data_opt_out_form.pdf
Contact: https://www.infopay.com/help.php
Notes: Print form, complete, and mail to listed address or fax to 888-446-1229.

Service: Infospace
Website: infospace.com
Removal Link: infospace.intelius.com/optout.php
Contact: support@infospace.com, info@infospace.com
Notes: Online removal tool will complete the process.

Service: Infotracer
Website: infotracer.com
Removal Link: https://infotracer.com/optout/
Contact: https://members.infotracer.com/customer/help
Notes: Online removal tool will complete the process.

Service: Instant Check Mate
Website: instantcheckmate.com
Removal Link: instantcheckmate.com/optout
Contact: privacy@instantcheckmate.com, support@instantcheckmate.com
Notes: Online removal tool will complete the process.

Service: InstantPeopleFinder
Website: https://www.instantpeoplefinder.com/
Removal Link: https://www.intelius.com/optout
Contact: support@instantpeoplefinder.com
Notes: Online removal tool will complete the process.

Service: Intelius
Website: intelius.com
Removal Link: www.intelius.com/optout.php
Contact: privacy@intelius.com
Notes: Online removal tool will complete the process.

Service: IntelligenceX
Website: https://intelx.io/
Removal Link: None
Contact: https://intelx.io/abuse
Notes: Online contact option will complete the process.

Service: John Doe
Website: johndoe.com
Removal Link: https://johndoe.com/optout_request
Contact: info@JohnDoe.com
Notes: Online removal tool will complete the process.

Service: Kiwi Searches
Website: https://kiwisearches.com
Removal Link: https://kiwisearches.com/optout
Contact: support@kiwisearches.com
Notes: Email request required.

Service: Lead Ferret
Website: leadferret.com
Removal Link: None
Contact: removeme@leadferret.com
Notes: Email request required.

Service: LexisNexis/Accurint
Website: lexisnexis.com
Removal Link: https://optout.lexisnexis.com
Contact: privacy.information.mgr@lexisnexis.com
Notes: Online removal tool will complete the process. You can upload digital documents.

Service: LexisNexis Direct Marketing
Website: www.lexisnexis.com
Removal Link: www.lexisnexis.com/privacy/directmarketingopt-out.aspx
Contact: privacy.information.mgr@lexisnexis.com
Notes: Online removal tool will complete the process.

Service: LexisNexis People Locator
Website: lexisnexis.com
Removal Link: None
Contact: remove@prod.lexisnexis.com
Notes: Follow instructions at lexis-nexis.com/clients/iip/removingInfo.htm

Service: Locate Family
Website: https://www.locatefamily.com
Removal Link: https://www.locatefamily.com/removal.html
Contact: https://www.locatefamily.com/contact.html
Notes: Online removal tool will complete the process.

Service: MashPanel
Website: http://www.mashpanel.com/
Removal Link: http://www.mashpanel.com/remove.php
Contact: http://www.mashpanel.com/contact-us
Notes: Online removal tool will complete the process.

Service: Mastercard
Website: mastercard.us
Removal Link: mastercard.us/en-us/about-mastercard/what-we-do/privacy/data-analytic-opt-out.html
Contact: None
Notes: Online removal tool will complete the process.

Service: Melissa Data
Website: melissadata.com
Removal Link: None
Contact: paul.nelson@melissa.com or brett.mcwhorter@melissa.com
Notes: Send email with removal request.

Service: Moment Verify
Website: momentverify.com
Removal Link: None
Contact: support@momentverify.com
Notes: Send email with removal request.

Service: MyHeritage
Website: http://myheritage.com
Removal Link: None
Contact: support@myheritage.com
Notes: Send email with removal request.

Service: My Relatives
Website: https://www.myrelatives.com/
Removal Link: https://www.myrelatives.com/manage
Contact: https://www.myrelatives.com/contact
Notes: Online removal tool will complete the process.

Service: MyLife
Website: www.mylife.com
Removal Link: None
Contact: privacy@mylife.com
Notes: Send email with removal request.

Service: Neighbor Report
Website: neighbor.report
Removal Link: https://neighbor.report/remove
Contact: support@ gew3.org
Notes: Online removal tool will complete the process.

Service: Number 2 Name
Website: www.number2name.com
Removal Link: http://members.infotracer.com/tspec/shared/assets/data_opt_out_form.pdf
Contact: None
Notes: Complete Infotracer Opt-out.

Service: Numberville
Website: https://numberville.com
Removal Link: https://numberville.com/opt-out.html
Contact: https://numberville.com/contact.html
Notes: Online removal tool will complete the process.

Service: Nuwber
Website: www.nuwber.com
Removal Link: nuwber.com/removal/link
Contact: support@nuwber.com
Notes: Online removal tool will complete the process.

Service: Old Friends
Website: https://old-friends.co/
Removal Link: https://old-friends.co/
Contact: support@old-friends.co
Notes: Online removal tool will complete the process.

Service: Old Phone Book
Website: http://www.oldphonebook.com/
Removal Link: None
Contact: paulmfield@gmail.com / lookupuk@gmail.com
Notes: Send request via email.

Service: PCCare99
Website: https://pccare99.com
Removal Link: None
Contact: panchamithracreators@gmail.com
Notes: Send email with removal request.

Service: PeekYou
Website: peekyou.com
Removal Link: www.peekyou.com/about/contact/optout/
Contact: support@peekyou.com
Notes: Online removal tool will complete the process.

Service: Peep Lookup
Website: https://www.peeplookup.com
Removal Link: https://www.peeplookup.com/opt_out
Contact: hello@peeplookup.com
Notes: Online removal tool will complete the process.

Service: People By Name
Website: www.peoplebyname.com
Removal Link: www.peoplebyname.com/remove.php
Contact: support@peoplebyname.com
Notes: Online removal tool will complete the process.

Service: People By Phone
Website: https://www.peoplebyphone.com
Removal Link: https://www.peoplebyphone.com/removal/
Contact: support@peoplebyphone.com
Notes: Online removal tool will complete the process.

Service: People Finder
Website: peoplefinder.com
Removal Link: peoplefinder.com/optout.php
Contact: support@peoplefinder.com, info@peoplefinder.com
Notes: Online removal tool will complete the process.

Service: People Finders
Website: peoplefinders.com
Removal Link: https://www.peoplefinders.com/manage
Contact: support@peoplefinders.com
Notes Online removal tool will complete the process.

Service: People Looker
Website: peoplelooker.com
Removal Link: www.peoplelooker.com/f/optout/search
Contact: west.privacypolicy@thomson.com
Notes: Online removal tool will complete the process.

Service: People Lookup
Website: peoplelookup.com
Removal Link: None
Contact: support@peoplelookup.com, info@peoplelookup.com
Notes: Send your custom opt-out request form via fax to 425-974-6194

Service: People Maven
Website: peoplemaven.com
Removal Link: https://goo.gl/forms/d2gQFkNqXBoblYKP2
Contact: support@peoplemaven.com, info@peoplemaven.com
Notes: Online removal tool will complete the process.

Service: People-Records
Website: https://people-record.com/
Removal Link: https://federal-data.com/control/profile?url=
Contact: https://federal-data.com/page/contact
Notes: Paste your original url from people-records.com following the = sign in the removal link.

Service: People-Search
Website: https://www.people-search.org
Removal Link: (Embedded in results)
Contact: info@people-search.org
Notes: Online removal tool will complete the process.

Service: People Search Expert
Website: https://www.peoplesearchexpert.com
Removal Link: (Appears on result page)
Contact: support@ peoplesearchexpert.com, info@ peoplesearchexpert.com
Notes: Online removal tool will complete the process.

Service: People Search Now
Website: peoplesearchnow.com
Removal Link: https://www.peoplesearchnow.com/opt-out
Contact: support@peoplesearchnow.com, info@peoplesearchnow.com
Notes: Complete form and mail to listed address.

Service: People Search Site
Website: https://www.peoplesearchsite.com/
Removal Link: Embedded in profile
Contact: info@peoplesearchsite.com
Notes: Click the opt-out link (bottom right of profile), and follow instructions.

Service: People Smart
Website: peoplesmart.com
Removal Link: www.peoplesmart.com/optout-go
Contact: privacy@peoplesmart.com
Notes: Online removal tool will complete the process.

Service: People Trace UK
Website: www.peopletraceuk.com
Removal Link: www.peopletraceuk.com/Record_Removal_Request.asp
Contact: support@peopletraceuk.com
Notes: Online removal tool will complete the process.

Service: People's Check
Website: https://www.peoplescheck.com
Removal Link: https://www.peoplescheck.com/optout/index
Contact: support@peoplescheck.com
Notes: Online removal tool will complete the process.

Service: People Whiz
Website: https://www.peoplewhiz.com
Removal Link: https://www.peoplewhiz.com/remove-my-info
Contact: info@PeopleWhiz.com
Notes: Online removal tool plus email confirmation will complete the process.

Service: Persopo
Website: www.persopo.com
Removal Link: None
Contact: support@persopo.com
Notes: Send email with removal request. Removes data from several subsidiaries.

Service: Persvera
Website: https://persvera.com
Removal Link: https://federal-data.com/control/profile?url=
Contact: https://federal-data.com/page/contact
Notes: Paste your original url from persvera.com following the = sign in the removal link.

Service: Phone Addresses
Website: https://phone-address.com
Removal Link: Click the trashcan icon to the right of your entry
Contact: None
Notes: Click the trashcan icon to the right of your entry

Service: Phone Detective
Website: https://www.phonedetective.com/
Removal Link: https://www.beenverified.com/app/optout/search
Contact: privacy@phonedetective.com
Notes: Online removal tool will complete the process.

Service: Phone Number Data
Website: http://www.phonenumberdata.net/
Removal Link: None
Contact: phonenumberdata@live.com
Notes: Send email with removal request.

Service: Phone Owner
Website: phoneowner.com
Removal Link: None
Contact: customer-service@phoneowner.com
Notes: Send email with removal request. Removes data from several subsidiaries.

Service: Phone Search Free
Website: www.phonesearchfree.com
Removal Link: www.phonesearchfree.com/opt-out
Contact: support@phonesearchfree.com
Notes: Online removal tool will complete the process.

Service: Phonebook (BT)
Website: www.thephonebook.bt.com/person/
Removal Link: www.productsandservices.bt.com/consumer/edw/privacypolicy/copyform/bt/#/
Contact: support@ productsandservices.bt.com
Notes: Online removal tool will complete the process.

Service: Property Shark
Website: https://www.propertyshark.com/
Removal Link: None
Contact: support@propertyshark.com
Notes: Send email with removal request.

Service: Private Eye
Website: https://www.privateeye.com/
Removal Link: https://www.privateeye.com/static/view/contact/
Contact: support@peoplefinders.com
Notes: Send email with removal request.

Service: Public Data Digger
Website: https://publicdatadigger.com/
Removal Link: https://publicdatadigger.com/removeprofile
Contact: support@ publicdatadigger.com
Notes: Online removal tool will complete the process.

Service: Public Data USA
Website: https://publicdatausa.com
Removal Link: https://publicdatausa.com/optout.php
Contact: https://publicdatausa.com/contact.php
Notes: Online removal tool will complete the process.

Service: Public Info Services
Website: https://www.publicinfoservices.com/
Removal Link: None
Contact: support@publicinfoservices.com
Notes: Send email with removal request.

Service: Public Mail Records
Website: publicemailrecords.com
Removal Link: None
Contact: publicemailrecords@gmail.com
Notes: Send email with removal request. Removes data from several subsidiaries.

Service: Public Records
Website: publicrecords.directory
Removal Link: https://publicrecords.directory/contact.php
Contact: support@ publicrecords.directory
Notes: Send email with removal request. Removes data from several subsidiaries.

Service: Public Records Now
Website: https://www.publicrecordsnow.com/
Removal Link: https://www.publicrecordsnow.com/static/view/optout/
Contact: https://www.publicrecordsnow.com/static/view/contact/
Notes: Online removal tool will complete the process.

Service: Public Records 360
Website: publicrecords360.com
Removal Link: publicrecords360.com/optout.html
Contact: optout@publicrecords360.com, privacy@ publicrecords360.com
Notes: Complete opt-out form and email with ID to optout@publicrecords360.com.

Service: Public Records Search
Website: https://www.publicrecords.com/
Removal Link: https://secure.publicrecords.com/emailcontact.php
Contact: https://secure.publicrecords.com/emailcontact.php
Notes: Send email with removal request.

Service: Public Seek
Website: https://publicseek.com/
Removal Link: None
Contact: privacy@publicseek.com & support@publicseek.com
Notes: Send email with removal request.

Service: Publishers Clearing House
Website: pch.com
Removal Link: None
Contact: privacychoices@pchmail.com
Notes: Send email with name and address and request to be removed from all databases.

Service: Radaris
Website: radaris.com
Removal Link: https://radaris.com/control/privacy
Contact: support@radaris.com, info@radaris.com
Notes: Select your profile and submit to removal URL.

Service: Reveal Name
Website: https://www.revealname.com
Removal Link: https://www.revealname.com/opt_out
Contact: support@ revealname.com
Notes: Online removal tool will complete the process.

Service: Reverse Phone Lookup
Website: www. reversephonelookup.com
Removal Link: reversephonelookup.com/remove.php
Contact: support@reversephonelookup.com, info@reversephonelookup.com
Notes: Online removal tool will complete the process.

Service: Sales Spider
Website: salespider.com
Removal Link: None
Contact: support@salespider.com
Notes: Locate profile and select "Delete this profile".

Service: Search Bug
Website: https://www.searchbug.com/
Removal Link: https://www.searchbug.com/peoplefinder/how-to-remove.aspx
Contact: support@searchbug.com
Notes: Follow online instructions at https://www.searchbug.com/peoplefinder/how-to-remove.aspx

Service: Search People Free
Website: https://www.searchpeoplefree.com
Removal Link: https://www.searchpeoplefree.com/opt-out
Contact: https://www.searchpeoplefree.com/contact-us
Notes: Online removal tool will complete the process.

Service: Smart Background Checks
Website: https://www.smartbackgroundchecks.com
Removal Link: https://www.smartbackgroundchecks.com/optout
Contact: https://www.smartbackgroundchecks.com/contact
Notes: Online removal tool will complete the process.

Service: Social Catfish
Website: https://socialcatfish.com
Removal Link: https://socialcatfish.com/opt-out/
Contact: welcome@socialcatfish.com
Notes: Online removal tool will complete the process.

Service: Spy Dialer
Website: www.spydialer.com
Removal Link: www.spydialer.com/optout.aspx
Contact: support@spydialer.com
Notes: Online removal tool will complete the process.

Service: Spokeo
Website: spokeo.com
Removal Link: www.spokeo.com/optout
Contact: support@spokeo.com, customercare@spokeo.com
Notes: Online removal tool will complete the process.

Service: SpyFly
Website: https://www.spyfly.com
Removal Link: https://www.spyfly.com/help-center/remove-info
Contact: support@spyfly.com
Notes: Sens email requesting removal.

Service: Spytox
Website: www.spytox.com
Removal Link: https://www.spytox.com/opt_out
Contact: hello@spytox.com
Notes: Online removal tool will complete the process.

Service: State Records
Website: https://staterecords.org/
Removal Link: https://infotracer.com/optout/
Contact: support@staterecords.org
Notes: Online removal tool for InfoTracer will complete the process.

Service: Super Pages
Website: www.superpages.com
Removal Link: https://www.whitepages.com/suppression_requests
Contact: support@superpages.com, info@superpages.com
Notes: "Remove from Directory" at the footer of the page

Service: Sync Me
Website: Sync.me
Removal Link: sync.me/optout/
Contact: ken@sync.me
Notes: Online removal tool will complete the process.

Service: Telephone Directories
Website: https://www.telephonedirectories.us/
Removal Link: https://www.telephonedirectories.us/Edit_Records
Contact: https://www.telephonedirectories.us/Contact
Notes: Online removal tool will complete the process.

Service: Tenn Help
Website: https://www.tennhelp.com
Removal Link: https://www.tennhelp.com/public-resources/change-listing.html
Contact: https://www.tennhelp.com/public-resources/contact-us.html
Notes: Online removal tool will complete the process.

Service: That's Them
Website: thatsthem.com
Removal Link: thatsthem.com/optout
Contact: Unknown
Notes: Online removal tool will complete the process.

Service: The Identity Pages
Website: http://theidentitypages.com/
Removal Link: http://theidentitypages.com/Remove
Contact: http://theidentitypages.com/ContactUs
Notes: Online removal tool will complete the process.

Service: Thomson/Westlaw/CLEAR
Website: thomson.com
Removal Link: None
Contact: west.privacypolicy@thomson.com
Notes: Send email with removal request.

Service: TLO
Website: https://tlo.com
Removal Link: None
Contact: CustomerSupport@TLO.com, TLOxp@transunion.com
Notes: Send demand via email to remove all records. Expect resistance.

Service: Tower Data
Website: www.towerdata.com
Removal Link: dashboard.towerdata.com/optout/
Contact: privacy@towerdata.com
Notes: Online removal tool will complete the process.

Service: True Caller
Website: https://www.truecaller.com
Removal Link: https://www.truecaller.com/unlisting
Contact: support@truecaller.com, info@truecaller.com
Notes: Online removal tool will complete the process.

Service: True People Search
Website: https://www.truepeoplesearch.com
Removal Link: https://www.truepeoplesearch.com/removal
Contact: https://www.truepeoplesearch.com/contact
Notes: Online removal tool will complete the process.

Service: Trustoris
Website: https://trustoris.com/
Removal Link: https://federal-data.com/control/profile?url=
Contact: https://federal-data.com/page/contact
Notes: Paste your original url from trustoris.com following the = sign in the removal link.

Service: Truth Finder
Website: https://www.truthfinder.com
Removal Link: https://www.truthfinder.com/opt-out/
Contact: support@truthfinder.com
Notes: Online removal tool will complete the process.

Service: UFind
Website: https://ufind.name
Removal Link: None
Contact: support@ufind.name
Notes: Send email with removal request. Removes data from several subsidiaries.

Service: United States Phonebook
Website: http://www.unitedstatesphonebook.com/
Removal Link: None
Contact: paulmfield@gmail.com / lookupuk@gmail.com
Notes: Send email with removal request. Removes data from several subsidiaries.

Service: USA People Search
Website: https://www.usa-people-search.com
Removal Link: https://www.usa-people-search.com/manage/
Contact: https://www.usa-people-search.com/contact.aspx
Notes: Online removal tool will complete the process.

Service: US Identify
Website: usidentify.com
Removal Link: None
Contact: privacy@peoplesmart.com
Notes: Send custom opt-out form to address on privacy policy page.

Service: US Phonebook
Website: www.usphonebook.com
Removal Link: www.usphonebook.com/opt-out
Contact: support@usphonebook.com
Notes: Online removal tool will complete the process.

Service: Valassis/RetailMeNot /Redplum
Website: https://www.retailmenot.com
Removal Link: https://www.retailmenot.com/everyday/unsubscribe
Contact: https://help.retailmenot.com/s/contactsupport
Notes: Online removal tool will complete the process.

Service: Valid Number
Website: https://validnumber.com/
Removal Link: None
Contact: https://validnumber.com/doc/contact/
Notes: Send removal request through contact page.

Service: Valpak/Cox
Website: Valpak.com
Removal Link: https://www.valpak.com/coupons/show/mailinglistsuppression
Contact: info@skulocal.com
Notes: Online removal tool will complete the process.

Service: Vehicle History
Website: https://www.vehiclehistory.com
Removal Link: None
Contact: support@ vehiclehistory.com
Notes: Email requesting removal.

Service: VeriGround
Website: https://veriground.com/
Removal Link: https://federal-data.com/control/profile?url=
Contact: https://federal-data.com/page/contact
Notes: Paste your original url from veriground.com following the = sign in the removal link.

Service: Veripages
Website: https://veripages.com
Removal Link: https://veripages.com/page/contact
Contact: support@veripages.com
Notes: Send email with removal request.

Service: Verispy
Website: https://www.verispy.com/
Removal Link: https://www.dataaccessmanagement.com/verispy/
Contact: support@verispy.com
Notes: Online removal tool will complete the process.

Service: Veritora
Website: https://veritora.com/
Removal Link: https://federal-data.com/control/profile?url=
Contact: https://federal-data.com/page/contact
Notes: Paste your original url from veritora.com following the = sign in the removal link.

Service: Visa
Website: http://visa.com/
Removal Link: https://marketingreportoptout.visa.com/OPTOUT/request.do
Contact: None
Notes: Online removal tool will complete the process.

Service: Voter Records
Website: https://voterrecords.com/
Removal Link: https://voterrecords.com/faq
Contact: https://voterrecords.com/contact
Notes: Follow directions in the FAQ above.

Service: Westlaw
Website: www.thomsonreuters.com
Removal Link: https://static.legalsolutions.thomsonreuters.com/static/pdf/opt_out_form.pdf
Contact: westlaw.privacypolicy@thomsonreuters.com
Notes: Print form, complete, and mail to listed address. Include extended opt-out form.

Service: White Pages
Website: whitepages.com
Removal Link: http://www.whitepages.com/suppression_requests
Contact: support@whitepages.com
Notes: Online removal tool will complete the process.

Service: Whoodle
Website: whoodle.com
Removal Link: None
Contact: support@whoodle.com
Notes: Send email with removal request.

Service: WYTY
Website: wyty.com
Removal Link: https://www.wyty.com/remove/
Contact: privacy@wyty.com
Notes: Online removal tool will complete the process.

Service: XLEK
Website: https://www.xlek.com/
Removal Link: https://www.xlek.com/optout.php
Contact: https://xlek.com/contact.php
Notes: Online removal tool will complete the process.

Service: Yasni
Website: yasni.com
Removal Link: None
Contact: info@yasni.com, support@yasni.com
Notes: No removal option, but will identify sources of data. Will refresh occasionally.

Service: Yellow Pages
Website: www.yellowpages.com/reversephonelookup
Removal Link: https://corporate.thryv.com/privacy-CCPA
Contact: ypcsupport@yp.com, press@yp.com
Notes: Online removal tool will complete the process.

Service: Zabasearch
Website: zabasearch.com
Removal Link: None
Contact: info@zabasearch.com, response@zabasearch.com
Notes: Send your custom opt-out request form via fax to 425-974-6194.

Service: ZoomInfo
Website: zoominfo.com
Removal Link: None
Contact: info@zoominfo.com, support@zoominfo.com
Notes: Click "Is this you?" in your profile. Signup and delete desired details.

Now that you have removed yourself from the public-facing databases, you may want to know what the private data mining companies store about you. The following resources allow you to demand your own reports displaying the details possessed by each company. You can notify each company if you see inaccurate details which should be omitted.

Service: Chex Systems
Website: chexsystems.com
Link: chexsystems.com/web/chexsystems/consumerdebit/page/requestreports/consumerdisclosure
Email Address: info@chexsystems.com
Notes: Submit the online form.

Service: Experian Rent Bureau
Website: experian.com
Request Link: https://www.experian.com/assets/rentbureau/general/request_form.pdf
Email Address: info@experian.com
Notes: Print and mail the form.

Service: LexisNexis
Website: lexisnexis.com
Request Link: personalreports.lexisnexis.com/pdfs/CD107_CP-File-Disclosure-Request-Form_pg-3.pdf
Email Address: info@lexisnexis.com
Notes: Print and mail the form.

Service: LexisNexis
Website: lexisnexis.com
Request Link: lexisnexis.com/privacy/for-consumers/CD307_Accurint_Person_Report_Info_Form.pdf
Email Address: info@lexisnexis.com
Notes: Print and mail the form.

Service: Medical Information Bureau
Website: mib.com
Request Link: https://www.mib.com/disclosuretransfer/disclosureservice/formrequest
Email Address: info@mib.com
Notes: Submit the online form.

Service: National Consumer Telecom and Utilities Exchange
Website: nctue.com
Request Link: https://www.nctue.com/Consumers
Telephone Number: 1-866-349-5185
Notes: Call and request report via mail.

Service: Retail Equation (Fraud Reports)
Website: theretailequation.com
Request Link: None
Email Address: ReturnActivityReport@TheRetailEquation.com
Notes: Email requesting a "Return Activity Report", include your name and phone number.

Service: Safe Rent (Core Logic)
Website: corelogic.com
Request Link: www.corelogic.com/downloadable-docs/nbd03-104-disclosure-request-web-packet.pdf
Email Address: info@corelogic.com
Notes: Print and mail the form.

Service: Tenant Data
Website: tenantdata.com
Request Link: https://tenantdata.com/file_download/25798b52-bcf6-4d09-ab38-04c6fbdfad7d
Email Address: info@ tenantdata.com
Notes: Print and mail the form.

Service: Westlaw (CLEAR)
Website: thomsonreuters.com
Request Link: https://static.legalsolutions.thomsonreuters.com/static/pdf/info_request_form.pdf
Email Address: info@ thomsonreuters.com
Notes: Print and mail the form.

Data Removal Shaming

In 2019, I began seeing more people search websites shaming those who have requested removal from their service. Consider the "Removal Error" page located on the Locate Family website at https://www.locatefamily.com/removal-errors.html. It publicly displays every person who requested removal while using a disposable or temporary email address. Not only did Locate Family refuse to remove the profiles, they announced to the world anyone who tried to protect their privacy by using a masked email provider. This is deliberately malicious and an attempt to shame anyone craving privacy. We must always be cautious of these abuses. If a site refuses to remove profiles because a masked email was used, we may need to assign a ProtonMail account for this purpose.

Social Media Background Services

In 2020, I began seeing more companies providing a service to report "inappropriate" workplace behavior as an employee screening strategy. If you are about to hire a person at your business, these companies will provide a complete report of online activity from the potential employee. This includes any social network posts which contain profanity or threats of violence. Unfortunately, these systems also collect posts with no inappropriate content. This is especially true with posts containing humor and sarcasm taken out of context.

One of the offenders in this game is FAMA (fama.io). It appears that they collect any publicly available social network content which displays "toxic behavior" and stores it indefinitely. When a potential employer requests this service and provides any identifiers about the employee, FAMA conducts a query and provides any content gathered about the individual. This usually includes posts which the employee "liked" which happen to contain a curse word. This seems quite excessive to me. If you identify any of these services in use by your potential employer, you might consider removing your data before the background check. Below are a few options for the most popular services.

- FAMA: Send an email to privacy@fama.io and specifically demand removal of any data stored in reference to your social network account(s).
- Social Intelligence: Send an email to info@socialintel.com or call 888-748-3281 and demand removal of any data stored in reference to your social network account(s).
- JDP: Send an email to clientservices@jdp.com or call 877-745-8525 and demand removal of any data stored in reference to your social network account(s).

If any of these companies refuse to honor your removal request, consider an additional attempt citing the California Consumer Privacy Act, as explained next.

California Consumer Privacy Act

In 2020, the California Consumer Privacy Act (CCPA) became effective, which is a state statute intended to enhance privacy rights and consumer protection for residents of California. However, residents of other states may also benefit from this law. First, let's summarize the basic characteristics of the CCPA. Overall, it grants California residents the following three basic rights in association to their relationships with businesses.

- KNOW what personal information companies possess about you.
- DELETE your information if desired.
- DEMAND companies not to sell your information.

This may sound powerful, and it is, but there are always caveats. First, you must be a California resident in order to be eligible for protections from this law. However, many companies with a strong California presence, such as Facebook, Google, Microsoft, and others are applying the protections to all customers regardless of location. Next, there are exemptions which companies can use to refuse your requests, including the following.

- The data is necessary to complete transactions.
- The data is necessary to comply with legal obligations.
- The data is necessary to protect security and functionality.
- The data is necessary to protect free speech.
- The data is necessary to complete scientific research.
- The data is necessary to complete internal uses.

It would not take much effort for a company to apply one of these exemptions to your request. However, it is always worth trying. In early 2020, I encountered a website which refused to remove sensitive personal information from their publicly available online service. I sent the following request to the email address on their website.

Pursuant to the California Consumer Privacy Act (CCPA), I demand that my personal information be removed from your website. Furthermore, per Part 4 of Division 3 of the California Civil Code (AB-375), I demand a waiver of any payment for this demand. My current California address is as follows.

Michael Bazzell
GENERAL DELIVERY
Los Angeles, CA 90001-9999

The company did not respond, but my information was removed the next day. They could have likely claimed an exemption, but it is less effort to simply remove content. It is also not worth the risk of violating the CCPA, as each violation carries a $2,500 - $7,500 penalty. This only applies when the company generates more than $25 million per year in revenue; collects information on more than 50,000 consumers each year; or derives more than 50 percent of its annual revenue from data. This should be applicable to most services which possess threats to our privacy.

I highly doubt the company displaying my details sent anything to the address I provided, but it is legal for me to use it. This address is the General Delivery option for Los Angeles, and any mailings will be forwarded to the post office located at 7101 South Central in Los Angeles. I would need to respond to that location with ID in order to pick up any general delivery mail. This should never be used whenever a package will be sent. I only use it as a temporary California address. I feel this is acceptable, as the official USPS website states "General Delivery is a mail service for those without a permanent address, often used as a temporary mailing address". Since my home is in the name of a trust, of which I am not the trustee, I believe I technically do not possess a "permanent mailing address". My PMB and UPS box would go away if I failed to renew either, so I view those as "temporary". I am probably unnecessarily splitting hairs here, but I like to have a clean conscious while executing my strange tactics.

The CCPA defines protected personal information as any data including the following.

Real Name
Alias Name
Postal Address
Email Address
Online Identifier
IP Address
Account Name
Social Security Number
Driver's License Number
Passport Number
Purchase History
Biometric information
Browsing History
Search History
Geolocation Data
Professional Information
Educational Information

This provides many opportunities for privacy seekers. Any time you identify a company possessing or selling this type of data about you, you might be able to demand them to stop. Each scenario will be unique, and you should expect resistance. I suspect we will see other states follow in California's footsteps. Ideally, we would see a federal law provide similar protections, but that is likely much more complicated than each state taking charge for their residents.

The United States Census

It may be useless documenting these strategies now, since we just experienced a census in 2020. The next tally of every resident in the country will not occur until 2030. However, we should have a conversation in the case that your neighborhood, city, county, or state decides to conduct their own investigation into the population within specific boundaries. A census is defined as the procedure of acquiring and recording information about the members of a given population. In simplest terms, the U.S. Census attempts to identify the primary residence of every resident as of April 1st every ten years.

The Census bureau will tell you that the responses are confidential and secure. The intentions are good, but we know the history of the government failing to protect our data, such as the OPM breach. They will want to know the full name, DOB, gender, and relationship of every person in your household. This may seem harmless, but we must use caution. If the Census bureau were to experience a data leak or breach, this content would be extremely valuable to the people search websites previously mentioned. If you applied the techniques in previous chapters in order to remove any association from your home to your name, you may be hesitant to hand these private details over to the government. Since it is federal law that you accurately complete the census form, there is no option to simply ignore this demand. If you do, expect Census employees to start knocking on your door demanding answers. Our goal is to stay off their radar, and not bring attention to ourselves.

However, you can comply with the Census while maintaining a sense of privacy. When you receive a form requesting the name, gender, and DOB of every resident of the home, I believe you can legally comply by responding similar to the following in the name fields.

Adult Male	Minor Male
Adult Female	Minor Female

This provides the number of occupants, gender, and whether each person is an adult or minor. This gives the Census enough data to continue their tally in order to provide appropriate services, grants, and various government programs to your area. If you do this, there is always a possibility that an employee will be unsatisfied with your answers and may still contact you to seek more information. I encourage you to include a VOIP telephone number on the form. This may encourage the employee to call instead of visiting in person. Most importantly, never lie on these forms or ignore them. This is not an opportunity to provide disinformation. Doing so may result in a steep fine.

Online Content Removal

Bad things happen. I know people who have spent many months creating their perfect invisible life only to see it jeopardized by one minor mistake. While this will likely never happen to you, it is important to be prepared. This section will provide immediate actions which can be taken to minimize the damage after a mistake or malicious act has caused a data leak. Your scenario will likely fall into one of the following categories.

- Your photo is posted online.
- Your financial information or documents are posted online.
- Your reputation is purposely slandered online.
- Your criminal or traffic charges are posted online.

Photo Leakage

If you strive to prevent photos of yourself from appearing online, you are aware of the constant struggle. Family and friends are constantly updating their Facebook, Twitter, and Instagram feeds with photo and video proof of every facet of their lives. There are no opt-out policies on these websites. There are no removal request forms. Your only option is a polite request.

I have found that a simple request to friends and family is usually sufficient for them to delete any sensitive photos. Unfortunately, there is little else that can be done. I can only recommend that you never take a threatening tone. This will only agitate the person that controls the photo and they may become resistant. I have found one thing in common with the majority of my clients with this problem. Every one of them had been tagged because of their own use of social networks. If you are not on Facebook, you cannot be tagged on Facebook. If you are not on Twitter or Instagram, you are much less likely to be seen on someone else's account.

In late 2015, I presented a keynote session at a large conference in the Caribbean. This 60-minute session focused on cyber-crime vulnerabilities and the ways that criminals use social media information to create sophisticated attacks. An hour later, I received an email from one of my automated alerts which monitor my personal information. An attendee in the audience had taken a photo of me during the lecture and posted it to Twitter. I immediately reached out through a private message and politely requested removal. The attendee agreed and the entire post was removed. This was completed before Google had the opportunity to add it to their images database. If I did not have a monitoring solution in place, which was Google Alerts at the time, I would never have noticed the post. Google and Bing would have indexed the post and image. I would then have a more difficult time removing all traces. Constant monitoring is vital.

Financial Information Leakage

If you find a page in a Google search result that displays personal information about you, such as your social security or credit card number, you can request immediate removal. Google will review the request and remove the information from their search results. This will not remove the information from the website that is displaying it, but it will take the link off Google to make it more difficult to find. Even if Google removes the link from their search results, you should contact the offending website directly and request removal of your information. The following are the three scenarios that will force Google to remove a link to personal information:

- Your Social Security Number is visible on a website.
- Your bank account or credit card number is visible on a website.
- An image of your handwritten signature is visible on a website.

Each of these situations can be reported through the following three specific websites:

- support.google.com/websearch/contact/government_number
- support.google.com/websearch/contact/bank_number
- support.google.com/websearch/contact/image_of_handwritten_signature

Each page will instruct you to complete an online form which requires your name, anonymous email address, the URL of the website that is exposing the information, the URL of a Google results page that displays the information, and the information being exposed. Fortunately, Google offers detailed help on these pages explaining how to obtain the required information.

Bing also offers an automated removal request with an option of "My private information (intimate or sexual imagery, credit card numbers, passwords)". This form can be found at the following website.

https://www.microsoft.com/en-us/concern/bing

In early 2015, I was contacted by an attorney that was attempting to remove some content from the internet. He and a former business partner had developed a nasty relationship after a failed venture. The former partner uploaded numerous sensitive contracts on which he claimed my client had defaulted. He placed them on his personal website and posted malicious comments about my client. Since my client had a very unique name, a Google search revealed this undesired information within the first three results. At first, I assumed that there was nothing I could do about this expression of free speech. The documents were legal.

However, each scanned contract on this website included the signature of my client. I submitted a request to Google for removal of the link to this website. I cited their policy about linking to images of a person's signature. Within five days, the link was gone. While the presence of a signature was not the concern of my client, I used it as leverage to remove the undesired content. Sometimes you may need to look at alternative ways to achieve your desired removal results.

If you want to know whether your signature, social security number, credit card number, or bank account information is visible on a public website, you will need to conduct specific searches. The easiest way is to occasionally conduct a search of your account numbers and view any results. Keep in mind that your searches will only be successful if the exposed data is in the same format of your search. Also, use an anonymous search option such as the website duckduckgo.com. You should conduct several searches of this type of data including spaces, without spaces, and only the last four or eight numbers alone. This also applies to searches for any financial account numbers and social security numbers.

Reputation Information Leakage

I constantly receive email messages asking for help with removal of slanderous content. This is usually from business owners trying to protect their brand; individuals wrapped up in online gossip; or parents attempting to shield their children from bullies. If someone simply states an opinion about your product or business online, there is nothing you can do. If someone is spreading rumors about you on social networks, no one will take your complaint. If you find malicious comments about your child online, you can only report it to the host of the content. However, there are a few "tricks" which can force content offline.

In 2015, I was contacted by a woman who was suffering from a bad case of stalking. Her ex-boyfriend constantly harassed her and her new boyfriend online. He posted malicious content on various websites and referenced them both by full name. He had posted so much content that some of it had made it to the front page of a Google search. At one point, the first result after searching her name was a pornographic video fictitiously claiming to be her. She had enough and wanted to take action.

These cases are sometimes difficult to tackle because of laws that protect free speech. I am obviously a big fan of the first amendment, but I also believe that one has a right to take advantage of other laws and policies in order to protect a reputation. My goal was to eliminate all malicious content from the first page of both a Google and Bing search. The following highlights my successes and failures.

The first website on her Google and Bing search results was a revenge pornography page. It displayed a pornographic video of an unknown female (not the victim) that appeared to be

asleep on a bed. An unknown man (not the suspect) then sexually molests the woman while she sleeps. It should be noted that this video was likely staged and the woman was probably a willing participant. These consensual videos have become popular on commercial pornography websites. The title of the video on this page included my victim's full name. The comments made several references to her, the new boyfriend, and her family. I believe that the former boyfriend wanted the world to think that the woman in the video was my victim. They did appear very similar physically.

Removing this first link was relatively simple. I first navigated to the official Google revenge porn reporting page at support.google.com/websearch/troubleshooter/3111061. I selected the following options, each of which appeared after the selection of the previous.

What do you want to do? Remove information you see in Google Search
The information I want removed is: In Google's search results and on a website
Have you contacted the site's webmaster? Yes, but they haven't responded
I want to remove: A pornographic site that contains a full name or business name
Does the page contain pornographic content? Yes
Does a full name or business name appear on the website without your permission? Yes
Does the page violate Google's Webmaster Quality Guidelines? Yes

I then supplied an alias email address that I created for the victim; the full name of the victim as it appeared on the web page; the address of the Google result page linking to the video; and the address of the actual video page. I submitted the request and moved on to Bing.

I navigated to Bing's simple "Report Content to Microsoft" website located online at https://www.microsoft.com/en-us/concern/revengeporn. I provided the victim's name as it appeared on the video page, the exact address of the page, confirmation that the victim did not consent to the posting, and a digital signature.

I received a response from Bing within 24 hours and the link was removed. Google responded over 15 days later and they also removed the link. Both cited their revenge porn policies and gave no resistance to the removal. While the female in the video was not the victim, I believe that identifying the victim as the participant warranted this type of submission. Interestingly, neither service specifically asked if the requestor was actually depicted in the pornographic video. They only required the requestor's name be included on the page.

At this point, the Bing results page was fairly clean. The first page included legitimate LinkedIn and other social network pages under the control of the victim. However, Google was a different story. The suspect had created a post on a popular revenge pornography web forum where he linked to the previously mentioned video. Technically, this video was not present on the website, only mention of it and a direct link. This forum post was now the number one

result when searching my victim's name. This page made several references to her full name and identified her in the inappropriate video. I submitted this page through the same Google reporting page and waited. I was denied the request because the page did not contain any actual pornography. The direct link did not satisfy the requirements of their takedown policy.

I took drastic action that would not be appropriate for all situations. This web forum allows any members to post comments about the videos. I created a new member account anonymously, and submitted a comment on the page in question. In this comment, I embedded an animated image in gif format that displayed a very short (partial) clip of the video in poor quality. This clip looped and repeats while people are reading the comment. It did not actually include nudity, only showing unidentifiable bodies from the target video. I re-submitted my request to Google and the link was removed nine days later, as it now violated their terms of service (even though it was my fault). The rest of the results on the first page of her Google search were legitimate websites that she approved. My work was complete.

Another victim in a similar scenario identified a website which contained extremely personal and slanderous content about her. The theme was that she was a cheater and it included false accusations of infidelity. She suspected it was published by her former boyfriend, as it appeared days after their breakup. It was a free WordPress blog hosted on the official WordPress domain. The page contained her full name and several photos of her. My first attempt was a DMCA takedown request, which failed.

DMCA is an acronym for the Digital Millennium Copyright Act. It is a U.S. copyright law. It addresses the rights and obligations of owners of copyrighted material who believe their rights under U.S. copyright law have been infringed, particularly on the Internet. DMCA also addresses the rights and obligations of OSP / ISP (Online / Internet Service Providers) on whose servers or networks the infringing material may be found.

My client confirmed that she possessed the original photographs which appeared on the website. Some of them were captured with her own mobile device, and her originals could prove this. In my view, she was the copyright holder of these images. WordPress was violating this since she did not authorize the publication of the photos. WordPress has an easy DMCA submission page at https://en.support.wordpress.com/our-dmca-process/. I followed the steps and issued my complaint. The next day, I received the following message.

"We have reviewed your DMCA notice and the material you claim to be infringing. However, because we believe this to be fair use of the material, we will not be removing it at this time. Please note that Section 107 of the copyright law identifies various purposes for which the reproduction of a particular work may be considered fair, such as criticism, comment, news reporting, teaching, scholarship, and research. Please note that you may be liable for damages

if you knowingly materially misrepresent your copyrights – and we may seek to collect those damages."

Not only did WordPress deny my claim, they threatened to seek damages from my submission. I am sure this is a canned response due to abuse, but I found it a bit inappropriate. My next attack was on the suspect blog itself. The page allowed anonymous comments below the slanderous content. I scribbled a barely legible signature on paper, took a photo with my anonymous mobile device, and uploaded it to the page. I then submitted the page to Google for takedown, per their policies about website containing signatures. It was gone from their index within a week. The original page is still present on WordPress, but no one searching for my victim will find it.

Libelous Websites

There is a disturbing new trend of websites which allow anonymous users to post any type of slander about an individual or company. These include services such as Ripoff Report and cheating spouse websites. Remember, it is not vital to always remove the CONTENT. It is more important to remove the LINK to the content from search engines. This is how people are likely to find the sites you want removed. I won't go to every website and look you up, but I will go to Google and follow any links. Therefore, I target the most likely source viewed by someone. Let's discuss complaint websites such as Ripoff Report as an example.

This website allows users to complain anonymously about any company or person. It requires users to create an account before reports can be submitted, but it does not verify the identity of users. Ripoff Report results usually show up on Google searches for the people or companies mentioned in the report, which can be embarrassing or damaging. According to the site's Terms of Service, users are required to affirm that their reports are truthful and accurate. However, the site says that it neither investigates, confirms, nor corroborates the accuracy of any submissions. In other words, it is an easy way to get revenge against an adversary.

Companies or individuals who have been named in a report may respond with a rebuttal. There is no charge to submit one, but they must have a registered account. The rebuttals are almost never successful in removal of information. Alternatively, to repair the reputation because of something that is written in the website, Ripoff Report asks victims to pay high fees for internal investigations of complaints and responses carried out by Ripoff Report's pool of arbitrators. Another way of phrasing this is "extortion". Again, these investigations almost never result in the desired removal.

How bad can these sites be? On Ripoff Report, I see entries about my clients falsely accusing them of fraud, adultery, theft, and in one instance murder. Anyone can post anything they

want without any accountability or fear of prosecution. It is a cesspool of hate. Worse are the "cheating" sites such as shesahomewrecker.com. These sites allow anyone to anonymously report a "cheater", including photos, full names, addresses, and explicit descriptions. These sites are a popular magnet for people desiring revenge, regardless if the other person has done anything wrong. There are also numerous websites that allow anonymous reporting of people that have a sexually transmitted disease (STD). For obvious reasons, I will not provide a link. Overall, there are many places where people can ruin digital lives quickly. Imagine if a Google search for your name instantly revealed a website announcing you have an STD. Clients call me constantly asking for help with these situations.

The best solution I have to offer is to attack through the legal system. Suing the websites is not likely to work in your favor. Many are hosted overseas, and all will claim protection by the 1996 Communications Decency Act which provides immunity from liability for providers and users of an "interactive computer service" who publish information provided by third-party users. In other words, I can host a website and not be held liable if someone else posts something defamatory.

Instead, I have initiated lawsuits in order to obtain a court order to remove online links to defamatory content. Google and Bing will not respond to my request to remove hateful content. Google may agree with me that the post is inappropriate, but that means nothing. They will only respond to a specific court order. Therefore, the first step is to get a judge to issue the order. However, that first requires a lawsuit. If you do not know the identity of the suspect, it can be difficult to launch a civil case. This is where a "John Doe" or "Fictitious Defendants" lawsuit can be a powerful tool.

Assume that Ripoff Report possesses an anonymous report about you. It clearly displays false defamatory content that has created a "loss" for you. Maybe you applied for a job and did not get it, and you believe it is from the posting. Maybe you have lost business because of the content. You may have significant losses which you can cite in court as damages. You file a fictitious defendant civil lawsuit at your local court due to the defamation and potential damages. This provides you subpoena power. You can now request a subpoena to the websites that possess the content with hopes of identifying the culprit via IP logs or email addresses. This identification rarely happens, but it places pressure on the sites and their legal teams.

Next, you can petition the court to provide an official court order to remove the content from the internet. The wording of this can vary, and must be precise to your situation. Be sure that the order forces removal of all links to the specified content and any cached copies. The offending sites will ignore this request, but Google will not. Upload the entire court order to Google at support.google.com/legal/contact/lr_courtorder?product=websearch.

Expect no response at first, and submit the same order once weekly until the links have been removed. Some courts will send the order on your behalf, which usually results in a faster removal. I have seen content removed within 48 hours and up to two weeks later. In most states, your right to file a defamation lawsuit ends a year after the initial publication, including original internet posts. In my experience, a John Doe suit can cost $5,000 to $15,000 in legal fees. Consult with an attorney to determine the relative merits and potential of success for your specific case. It is possible to do all of this yourself, but it is not advised. Any mistake can ruin your chances of an order being signed by a judge.

This court order is often in the form of a Cease and Desist order (not a letter). An order is created by the court, and a letter would be created by you. Cease and Desist letters are almost always ignored, but a court order is not. This universal document can be used in many scenarios, such as copyright infringement, trademark infringement, debt collection, harassment, slander, and libel. These orders vary widely between states, counties, and judges. Because the order is issued by the judge presiding over your civil case, you must convince him or her to issue the order, and to include the desired wording. This is where a well-known local attorney can be very valuable.

Any valid Cease and Desist court order should include descriptions of each false statement, reasoning why the statements are false, and descriptions of how the false statements affect you. You must clearly claim that you have damages from the published content. Without this, there is very little need for a civil suit. I have had clients who have been able to substantiate financial loss, even if minimal, from the undesired content. It will be up to you to determine if you have suffered any loss. The following page contains a fictitious example of a court order demanding Google to cease and desist providing access to libelous content. It is not a template or actual document, and is presented only for understanding of the technique.

Assume that you own a carpet cleaning company, and one of your competitors posted on Ripoff Report stating you were a criminal and possessed STDs (this is a common theme with libelous online complaints). The order on the following page would tackle this and demand that Google remove the links to this content.

I have over-simplified the process of filing a lawsuit and obtaining a court order. This is where a proficient attorney can assist greatly. I never attempt any of this myself. I always hire a local attorney on behalf of my client. I usually seek former prosecutors who understand the system and have direct access to judges.

CEASE AND DESIST ORDER

[The Honorable Judge John Doe]
[City, State, Zip Code]
[Date]
VIA Certified Mail

Google Inc.
Legal Compliance
1600 Amphitheatre Parkway
Mountain View, CA 94043

RE: Cease and Desist – Libel

To Whom It May Concern:

It has come to my attention that your company is currently providing direct access to specific online content contested as libelous to [YOUR NAME]. A direct link to the libelous website is available on your service when searching [YOUR NAME]. The exact address of this content is currently located at https://www.ripoffreport.com/reports/carpet-cleaning-by-psycho. The content on this page states in part:

"[YOUR NAME] is now facing multiple criminal and civil actions including investigation by the IRS and FBI for failure to pay taxes, impersonating a federal agent, making false claims, animal abuse, slander, fraud, stalking and collecting welfare funds while claiming no source of income. He is a pervert and has several STDs."

[YOUR NAME] contests these statements as false during current civil litigation. [YOUR NAME] has no known criminal record and there is no known evidence available to this court substantiating the additional claims made on this site. [YOUR NAME] claims economic harm as a result of the online content that your company provides during a search of the name [YOUR NAME]. [YOUR NAME] claims potential loss of income due to potential employers identifying this content during a search of [YOUR NAME].

I hereby demand that you immediately cease and desist displaying any hyperlinks, including any cached content, to the above referenced website(s) within 10 days of the date of this letter, and notify me in writing when these tasks have been completed.

_____

Judge John Doe

Criminal Information Leakage

Many new websites have appeared which host mugshots and associated criminal information of anyone arrested in select states. This varies based on state laws which allow unlimited access to this type of content. While arrest records are public data, I do not support websites that post this data in bulk. They are not doing this as a public resource. They are extortion websites which hope to benefit from your removal request. Most of these will remove your mugshot for $500. The only purpose for these sites is for financial gain.

I have found removal requests to these websites to be a waste of time. Letters from lawyers will go unanswered. They simply do not care. If your mugshot appears on one of these sites, I have only found two potential solutions. Your results will vary with this technique. The following examples will explain the processes that I took for two clients.

I was contacted by a subject who had been arrested for speeding. This may sound ridiculous, but he was speeding over 20 miles per hour above the limit, which was a misdemeanor in his state. He was booked, processed, and released on bond. The next day, his mugshot appeared on one of these extortion sites. Within a week, it had been indexed by Google. A search of his name revealed the mugshot directly above his LinkedIn and business websites. He was devastated.

The website that hosted this image was fairly dysfunctional. It was poorly designed and only existed to make a quick buck. I placed an alert on the exact page where the client's information was hosted through a service called Visual Ping. The moment that the website went down for maintenance, I received an alert that the page had changed. I immediately submitted a request for Google and Bing to re-index the client's mugshot page, which was offline. I identified the address as missing, and both Google and Bing re-indexed it during the 24-hour maintenance down-time.

The mugshot was no longer listed in his search results. If someone were to search the website directly, they could still see the photo. This is highly unlikely. It is possible that Google and Bing could re-index this live data. I have found that this usually happens when new content is posted. Since I informed the search engines that the content was missing, it will not immediately re-index that stale data.

I want to clarify that I was very lucky in this scenario. I took advantage of the situation. It is not a permanent solution, but it did buy some time to make an intentional decision that is not based on frantic thinking. I take a firm stance against paying the removal fees offered by these sites. Not only does it give in to this type of behavior, but it also increases the chance of the photo reappearing. If you paid once, you will likely pay twice. Furthermore, most of these websites are owned by the same entity.

The second solution takes advantage of new state laws specifically targeting mugshot websites. Lucky for nomads of South Dakota, this state possesses strong laws that demand these sites remove your content at your request. Send a certified letter to the website stating your demand to remove your mugshot from the website. Advise that this must be completed within 30 days, per South Dakota state law (or your state). Expect this demand to be ignored. After the 30 days has passed a small claims suit against the offending website should be considered. In my experience, this causes the website to remove the content in order to avoid a costly court appearance. They will know they are in violation of law and rarely submit any resistance.

Right to be Forgotten

The right to be forgotten is a concept that was discussed and put into practice in the European Union and Argentina in 2006. Search engines began to acknowledge this option in 2014. The issue has arisen from desires of individuals to determine the development of their life in an autonomous way, without being perpetually or periodically stigmatized as a consequence of a specific action performed in the past. Basically, you have the right to "start over" in Europe. This does not apply to Americans.

Google and Bing both allow you to submit requests for content removal from search engines if you live in Europe. The removal forms can be found on their support pages similar to the instructions mentioned in the previous example. They will ask for the search results URL and a digital signature of your name. They will verify that your name appears in the results and remove anything defamatory from the index.

Until recently, I found that submitting a request from an email address that possessed a UK domain was sufficient as proof of citizenship. However, Google has become much stricter and now demands photocopied identification. I have found Bing to be more lenient. I cannot advise you on how to proceed with a request like this if you do not live in Europe. I have received many success and failure stories from other people's attempts to take advantage of this law.

If your sensitive details are posted anywhere online, it is vital that you act quickly. The internet is a timer counting down until your data is spread onto additional websites. Proper alerts, constant monitoring, and better sharing habits will protect your privacy long term. I respect that we cannot control the internet and that removing personal data is like playing cat and mouse. However, I take my privacy seriously. I am willing to put in the effort in order to maintain my desired level of anonymity. Even as an author and international speaker, I keep a low profile online. I have two websites, but neither connect to my home address or telephone number. I have a business Twitter account, but no posts mention anything about my personality, interests, or location.

Proactive Online Content

The previous text summarized steps taken on behalf of clients to clean up after an unfortunate online post. Another powerful tactic is to populate desired content before there is need for it. If you create appropriate online content about yourself and promote it within search engines, it becomes more relevant to Google in terms of search results. The longer you "age" these pages, the more weight they hold when someone searches your name. The goal is to provide enough "good" online content so that the "bad" stuff is more difficult to find. I have found the following to provide the most impact toward an online search in your name.

Blogs: You can create free blogs on WordPress, Weebly, Wix, and other sites. Your blog should include your name and possibly vague or inaccurate location data. Consider a test example of michaelllezzab.wordpress.com. I created this page for free under the name of Michael Llezzab. If you search that full name, or a fictitious email address which I created of q9u7uaxbspas@opayq.com in Google, you should be linked to the blog(s). If a new website pops up with defamatory content about that name, it will likely appear beneath the results of my aged blog. The more activity within the blog, the higher the preference by search engines.

Websites such as ifttt.com can be configured to automatically populate content to your blog every day. You can see that my example blog receives updates automatically without any need to log in to it. This tells Google that the site is active and places priority over dormant sites. The following instructions will populate your current free WordPress blog with every new post created by another blog hosted at krebsonsecurity.com. This will result in a site similar to mine with constant new content, all automated behind the scenes.

- Create a free WordPress blog at wordpress.com. Supply your real name and any inaccurate details desired, such as a false telephone number and burner email address. Remain logged in to this account in your browser.
- Create a free account with If This Then That at ifttt.com. Search for "WordPress RSS" in the top search field and select the "RSS to WordPress" option. Click the "On" switch and it will ask for your WordPress credentials. Since this is a free throw away blog, I do not object to sharing this unique password. Save and enter a new feed item of "krebsonsecurity.com/feed". Save your entry.
- If you do not see the blog updates on the home page, make sure that "Your Latest Posts" is selected in the Settings > Customize > Homepage Setting menu.

Ideally, you will create numerous blogs, each with unique data populated daily by ifttt.com, which should force any undesired content to later pages in the search results. Another example is at https://michael-llezzab.weebly.com. In my experience, it can take many months before Google indexes these pages. Act now.

Domain: Purchasing a domain in your real name can have many benefits. Google tends to place more emphasis on private domains versus free blogs. It also reserves a specific domain, such as michaelbazzell.com, preventing someone else from buying it. Finally, it appears more credible than a free website outside of your control. Most of my clients are provided a domain name associated with their true name. This site then possesses minimal information such as full name and inaccurate location information. Occasionally, I place a resume with fictitious data on the site to throw off any stalkers. The opportunities for content are endless. Once it is complete, I connect it to Google's Webmaster Services in order to promote it on their search engine. This causes Google to index the site quicker and give it priority over some undesired content. I typically choose the lowest hosting and domain package from Namecheap for most clients. Currently, a domain and hosting for the first year can be purchased for $20.

LinkedIn: I normally stay away from social networks, but there are some use cases for LinkedIn. This was mentioned briefly earlier, but I will go into more detail here. If I have a client who has been the victim of constant harassment, I might use LinkedIn as a ruse. I will create an account in her name, publicly display her full name, and include enough accurate history which is already available online. This might include an old job if it is already posted somewhere else. Then, I specify a false location, such as New York City, and announce she is a student at a large university. While it may not fool her adversary, it might waste his time investigating these options.

Resume: I have posted numerous resumes which contain inaccurate details for my clients. I have found resumes to be constantly scanned and collected by recruiting services, and this quickly becomes populated online. In one scenario, I uploaded a resume in my client's name with a false telephone number, email address, and city of residence. This was replicated across 14 websites. Today, when you search her name, the first two pages of results are nonsense that does not expose her or display any negative statements. If someone decides to create a blog about her, it will be buried within these deliberate results.

Overall, the goal is to populate enough neutral content about yourself in order to suppress any potential negative postings. This is not a magic bullet. A good investigator will always dig through every search result. However, the casual internet searcher may not make it to any negative content. When you combine proactive online details and data removal into one overall privacy strategy, you have a powerful set of tools. You are more prepared for potential exposure and your experience will be better than that of someone who has not taken these actions.

Credit Freeze

Over the past ten years, I have conducted numerous presentations about digital crime to global audiences. The one question that I am asked more than any other during these events is "Should I purchase an identity protection service?". While this is a personal decision, I always disclose that I do not subscribe to any of these services. I have had a credit freeze for several years, and do not require expensive identity protection. I believe that those who have a credit freeze in place should not worry about their identity being stolen. Furthermore, I think that a credit freeze is better than the best identity monitoring product that will ever exist. I believe that every U.S. citizen should consider one. I will explain the submission process in a moment.

Protecting Your Credit Accounts & Debit Cards

If a criminal wants to get your money quickly and easily, he or she will target your debit and credit cards. Before the popularity of the internet, this required physical access to your wallet or purse. A victim would know right away that a card should be canceled and the damage would be minimal if caught early. A criminal would risk capture by attempting charges on the cards in person. Today, possession of your cards is not necessary. The internet has created a new avenue to obtain and spend the money in your accounts. This may occur without any indication of problems on your end. This section will present the tools that you need to protect your credit and make you practically invulnerable to identity theft.

Free Credit Report

Before I discuss the techniques that will protect you, you should take a good look at your current credit report. This will identify all of your current open accounts and may identify any problems or fraudulent activity. There are several websites that offer a free credit report. Most of these will try to convince you to sign up for premium offers and never offer an actual free credit report. The only official government-supported and truly free credit report website is at annualcreditreport.com. This website allows you to view your credit report, without any fee, once yearly from each of the three largest credit bureaus. This means that you actually can get three free credit reports every year. Instead of viewing all three reports at the same time, create a schedule to spread out the viewings. I recommend the following.

First, I recommend obtaining your entire credit report from Equifax online at their website https://www.annualcreditreport.com. This free report should be used to identify any unknown uses of your identity. If you do not want to submit the request online, you can use the form at https://www.annualcreditreport.com/manualRequestForm.action to mail in the submission.

I recommend that you consider closing any unused open credit accounts. The only exception would be whichever account has been opened the longest. If you have an unused account that has been open for ten years without any problems, you may consider leaving that account open. This will help your credit score, whereas closing your oldest account could decrease your score. Closing other unused accounts will provide fewer options for fraud. If you possess a credit line with a local bank that is never used, and that bank experiences an intrusion into their system, you may be victimized for weeks without knowing. The fewer open accounts that you have will result in fewer opportunities for financial fraud. Personally, my priority would be to close any specialty store accounts that you may have opened because of a sales discount, a free promotional item, or a pushy sales person.

Analyze your entire credit report for any errors. Occasional typos are common, and should not create panic. When I first viewed my own report, I discovered that someone else was using my social security number. I was immediately concerned and began to contact the credit bureaus. I quickly discovered that the "suspect" was someone with an SSN almost identical to mine, and someone had mistyped a number at some point. This will happen, and it is not an indication of fraud. You should focus on the open accounts. If you see that you possess a line of credit at an unfamiliar bank, then you should be concerned. If you discover anything suspicious, contact the credit bureau and financial institution to report the potential fraud. They all have a fraud division that will assist with identifying the problem and resolving it. Each situation will be unique and one vague example here would not necessarily apply to you.

You should also contact any financial institution that hosts the fraudulent account and notify them of the issue. You will be mailed paperwork to validate that the account was not opened by you. The process of closing the account will move quickly after that. If you do discover fraud on your credit report, I recommend that you immediately request your report from the other two credit bureaus. This may identify additional fraud that was not listed on the first bureau's report. If you do not discover fraud, I suggest that you wait a few months before you view the next report. This allows you to continuously monitor your credit throughout the year. Keeping an eye on your credit report is one of the most important tips that I mention in my public speaking appearances.

Credit Opt-Out

Under the Fair Credit Reporting Act (FCRA), the consumer credit reporting companies are permitted to include your name on lists used by creditors or insurers to make firm offers of credit or insurance that are not initiated by you. These are the pre-approved credit and insurance offers that you receive in the mail. They are often physically stolen by street criminals and submitted to receive a credit card in your name at their address. The FCRA also provides you the right to opt-out, which prevents consumer credit reporting companies from providing your credit file information to businesses.

Through the website optoutprescreen.com, you may request to opt-out from receiving such offers for five years. If you want to opt-out permanently, you can print a form that you must send through postal mail. If you choose to opt-out, you will no longer be included in offer lists provided by consumer credit reporting companies. The process is easy.

Credit Freeze Submission

During my training sessions, people often ask about paid services such as Lifelock and Identity Guard. They want to know how effective they are at protecting a person's identity. These services can be very effective, but you pay quite a premium for that protection. A more effective solution is a credit freeze. This service is easy, free, and reversible. A credit freeze, also known as a credit report freeze, credit report lock down, credit lock down, credit lock, or a security freeze, allows an individual to control how a U.S. consumer reporting agency is able to sell his or her data. This applies to six unique credit bureaus (Equifax, Experian, TransUnion, Innovis, Chex, and NCTUE). The credit freeze locks the data at the consumer reporting agency until an individual authorizes permission for the release of the data.

Basically, if your information stored by the credit reporting bureaus is not available, no institution will allow the creation of a new account with your identity. This means no credit cards, bank accounts, or loans will be approved. In many cases if someone tries to use your identity but cannot open any new services, they will find someone else to exploit. I can think of no better motivation to freeze your credit than knowing that no one can open new lines of credit in your name. This does NOT affect your current accounts or credit score.

A credit freeze also provides a great layer of privacy protection. If companies cannot gain access to your credit report, they cannot identify you as a pre-approved credit recipient. This will eliminate many offers mailed to your home. This will also remove you from various databases identifying you as a good credit card candidate. Credit freezes are extremely easy today thanks to State laws that mandate the credit bureaus' cooperation. This section will walk you through the process. Be sure to properly store any PINs provided to you (usually sent via mail) after the successful freezes. You will need this to un-freeze your credit if desired. As of March 2020, Equifax (and possibly others by now) no longer issue a PIN, and rely solely on responses to historical financial questions in order to lift a freeze.

Now that credit reports and freezes are free due to a new federal law, which can be researched online at www.congress.gov/bill/115th-congress/senate-bill/2155, I feel it is time to execute credit freezes in all possible locations. First, submit a credit freeze at the six current credit bureaus via their online submission, telephone, or postal mail options displayed within the following resources. I typically recommend clients begin with the online submission process and move to telephone or postal mail applications if anything is declined (which is common).

Equifax
Online: https://www.freeze.equifax.com
By Phone: 800-685-1111
By Mail: Equifax Security Freeze
PO Box 105788, Atlanta, Georgia 30348-5788

Experian
Online: https://www.experian.com/freeze/center.html
By Phone: 888-397-3742
By Mail: Experian Security Freeze
PO Box 9554, Allen, TX 75013

TransUnion
Online: https://service.transunion.com/dss/orderStep1_form.page
By Phone: 888-909-8872
By Mail: TransUnion LLC
PO Box 2000, Chester, PA 19016

Innovis
Online: https://www.innovis.com/personal/securityFreeze
By Phone: 800-540-2505
By Mail: Innovis Consumer Assistance
PO Box 26, Pittsburgh, PA, 15230-0026
https://www.innovis.com/assets/InnovisSecurityFreezeRequest-110141767716e41ac7d862e221ac5831.pdf

Chex
Online:
https://www.chexsystems.com/web/chexsystems/consumerdebit/page/securityfreeze/placefreeze/
By Phone: 800-887-7652
By Mail: Chex Systems, Inc. Attn: Security Freeze Department
7805 Hudson Road, Suite 100, Woodbury, MN 55125

NCTUE
Online: https://www.nctue.com/Consumers
By Phone: 866-349-5355
By Mail: NCTUE Security Freeze
PO Box 105561, Atlanta, GA 30348

After you have received confirmation that the six credit bureaus have placed a freeze on your credit, navigate back to https://www.annualcreditreport.com and request your free credit report from Experian. This report should acknowledge that a freeze is successfully in place. In a few months, repeat the process for Transunion. You are allowed one free report from each of the three providers every year.

Additional Credit Freeze Submissions

Since the publication of the previous edition of this book, several new data mining companies began offering credit freezes. While I believe everyone should consider a freeze with the previous six services, the following options are not as vital. Extreme privacy enthusiasts may desire their identities to be locked to their maximum potential. If you fit into that camp, then the following are for you.

Core Logic: You can obtain a credit freeze at the three services provided by Core Logic, including Credo, Rental Property Solutions, and Teletrack. Core Logic is an emerging provider of credit checks for third parties. I have never needed their services or approval, and likely never will. Therefore, I have frozen my profile within each of their offerings. The following websites will complete the process online.

Credco: https://credcofreeze.corelogic.com/
Rental Property Solutions: https://rpsfreeze.corelogic.com/
Teletrack: https://teletrackfreeze.corelogic.com/

Once a security freeze is in place, Core Logic will provide you with a PIN. Once frozen, your consumer file will only be released when you directly contact Core Logic, provide them with your personal PIN, and request that any information they have on you be released. If you need to lift the freeze temporarily for a period of time, you may request a temporary lift for all third parties by completing the initial request form on the websites mentioned above. Upon submission of your request, you will receive an email from Core Logic, requesting your basic information and your PIN. You can define the length of time you want your consumer file to be available. When that period ends, your files will be frozen again.

TALX: Please consider a freeze of your employment history maintained by The Work Number (Equifax). If any of your current or past employers contracted with this service for employment verification, any details you provided to the company were shared. If your employer did not query this service, you still likely possess a profile which includes your full name, address history, employment history, salary details, and other sensitive information. To place a security freeze on your The Work Number employment report, call them at 800-996-7566 or send a written request via mail to:

TALX Corporation
ATTN: Employment Data Report Dept 19-10
11432 Lackland Road
St. Louis, Missouri 63146

Sagestream: Formerly known as IDA, this company is aggressively entering the credit reporting market. Fortunately, their self-serve online freeze process is immediate and free. Visit https://www.sagestreamllc.com/security-freeze to file online or via postal mail. A PIN will be mailed to your verified address and can be used to temporarily lift a freeze if you seek credit from a company querying Sagestream. I have yet to see a need to remove this freeze once enacted.

Advanced Resolution Services: This service allows a temporary lift of a freeze through their website (https://ars-consumeroffice.com), but the initial request must be received via postal mail. You will need to send the same documentation required by the previous "big six" credit bureaus to the following address. Lately, I see very few companies querying this service, so you might consider skipping this one if you do not feel comfortable disclosing personal details to them.

Advanced Resolution Services
5005 Rockside Rd
Ste 600
Independence, OH 44131

PRBC: My advice here is a bit different from the previous options. I recommend that you first consider whether your data is currently stored by PRBC before taking any action. If you have been notified that smaller bureaus such as Innovis, Chex, or NCTUE do not possess a profile about you which can be frozen, then you may not have a presence at PRBC. If desired, you can request a copy of your credit report stored by PRBC before demanding a freeze. However, they demand unredacted copies of the front and back of your DL. This prevented me from demanding a copy of my data. The required data to freeze your profile is very demanding, and may not be appropriate for those in sensitive situations. Full details of both processes can be found at https://www.prbc.com/consumer-affairs.

I cannot stress the importance of credit freezes enough. Anyone with an SSN should submit one right away to all possible options. The new federal law also mandates that any child with an SSN under the age of 16 can also have a free credit freeze. I highly recommend locking down the credit of the entire family.

Several readers have been impacted by the huge breach at the Office of Personnel Management (OPM). Many of you have now received an official notification if your records were part of the breach. If you have ever held a clearance, or applied for one, you are likely a victim. The response from OPM is to offer temporary free credit monitoring. Unfortunately, if you already have a credit freeze in place, you cannot participate in the free coverage. Why? Your credit freeze is blocking the legitimate service from monitoring your activity. I believe that this speaks volumes about the effectiveness of a credit freeze. Aside from hackers, credit monitoring companies cannot see the details of a frozen account. I urge you to never remove a credit freeze in order to allow any free credit monitoring.

Many of these third-party credit monitoring services also induce people to provide even more information than was leaked in the original breach. For example, ID Experts (the company that OPM has paid $133 million to offer credit monitoring for the 21.5 million Americans affected by its breach) offers the ability to "monitor thousands of websites, chat rooms, forums and networks, and alerts you if your personal information is being bought or sold online". However, in order to use this service, users are encouraged to provide bank account and credit card data, passport and medical ID numbers, as well as telephone numbers and driver's license information.

I can see no reasonable purpose for ever giving any company more personal information in order to protect that same data. What happens when they get breached? On a personal note, I was a victim of the OPM breach. I am not worried. I have credit freezes in place, and they have been tested. I have no automated credit monitoring. Am I still vulnerable? Of course, we all are. However, I am a much more difficult target.

Fraud Alerts

In the previous edition of this book, I only placed emphasis on the credit freeze, and did not explain a credit fraud alert. This was intentional, as a freeze is much more powerful than an alert. A freeze prohibits a hard credit check while an alert simply asks a creditor to dig deeper into any requests. In other words, a freeze stops unauthorized credit pulls while a fraud alert slows them down. In 2020, I began recommending both credit freezes and fraud alerts if you want true protection from unauthorized credit accounts. This is because credit bureaus are slowly removing some of the protections of the credit freeze due to widespread adoption and the elimination of fees. Basically, people are freezing their credit in record numbers, which is causing headaches to the credit industry.

All three major credit bureaus offer fraud alerts without any charge. However, choosing the best option is not always clear. Each bureau offers an initial 1-year alert, extended 7-year alert, or 1-year active duty military alert. My preference is always the extended 7-year option, but there are requirements to qualify. In order to obtain the 7-year protection, you must be the

victim of "fraud" and must submit proof of this claim. Traditionally, this would be a police report of identity theft. However, I am aware of many people who cited various popular data breaches and submitted letters of notification from the breached companies. If you possess a police report of identity theft, this is always preferred. If not, I believe you should attempt a fraud alert by providing whatever documentation you have which supports fraud potential toward your credit. Once you have identified the documentation you will be sending, navigate to the following websites and select the 7-year extended fraud alert.

https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
https://www.experian.com/fraud/center.html
https://www.transunion.com/fraud-alerts

Follow the directions for each provider and wait for a mailed letter confirming activation of the alerts. Any time you seek a new line of credit, the credit bureau will apply more scrutiny toward your application, regardless of releasing a credit freeze. In early 2020, I applied for a new credit card as a test of my own security. The following details should explain why a fraud alert is necessary along with a credit freeze.

I have possessed a fraud alert through Equifax, Experian, and TransUnion since 2011. I renewed the alert in 2018. I always assumed it was unnecessary since I also possessed a credit freeze within all listed credit bureaus, but I like to push things whenever I can. I decided to apply for a new business credit card and knew the freeze would be a roadblock. I applied online for the card I wanted and expected a notice stating I had been declined, which happened right away. I was advised to place a call to customer support.

During the call, I was informed that my application had been declined due to the credit freeze. I intentionally applied with a freeze in place in order to test the security of the freeze itself. It passed the first test. The customer support employee told me I would need to release my freeze through Equifax in order to complete the application process. I played along, but also played dumb. I was directed to the Equifax credit freeze website which allowed an option to lift the freeze temporarily. However, I do not prefer this option during a credit card application.

Instead, I chose the option to grant a creditor a one-time code in order to access my credit report. This allows me to complete the application process without lifting the entire freeze for anyone else to abuse. It also prevents me from ensuring the re-freeze was properly executed. After selecting this option, I was presented a typical screen asking for personal details. I was also presented a field to enter my PIN assigned by Equifax during the credit freeze process. I was surprised to see an option to continue without providing a PIN.

While I knew my PIN, I selected the button that stated I did not know it. The customer support specialist confirmed that I would not need my PIN for this process. After providing my full name, physical address, DOB, and SSN, I was presented four "security questions" to verify my identity. These included selecting a known phone number, physical address, and previous employer. Afterward, I was presented a code to give to the credit card processor.

I want to pause here and vent my frustration. I placed a credit freeze in order to prevent anyone else from opening lines of credit in my name. I was mailed a PIN which would be required in order to lift the freeze. Instead, I was able to remove the freeze by supplying public information. My name, address, DOB, and SSN are available within numerous data breaches which are in the hands of criminals. The PIN was the only piece that was truly private, but it was bypassed by simply stating I did not possess it. The follow-up questions could have also been answered with publicly available data. The system is flawed. This is where a fraud alert can be beneficial.

After I gave the access code to the support representative, he was able to access my credit report. However, he could not complete the application due to my fraud alert with Equifax. This required him to verify additional information about me. He first asked me to identify the telephone number which I had attached to the fraud alert. I referenced my password manager which maintained these details and I provided the Google Voice number I had used during the fraud alert process. He confirmed it was correct. He then notified me that he would need to call me at that number.

We terminated the call, I logged in to my Yubikey-protected Google account, and answered the new incoming call to my "trusted" number. I again confirmed my name, address, DOB, and SSN over this new call, and the application was approved. Immediately after the call ended, I received a text message from a former colleague at the government building at which I previously worked. He told me that the credit card company had called asking for me, and thought I should know. Apparently, my old office number was also included on the "approved numbers" list.

I now believe that a credit freeze + fraud alert combination is the most protective solution in regard to preventing unauthorized access to your credit report. The freeze prevents a hard pull on your credit, but it can be defeated by a determined adversary. The fraud alert adds additional layers and should demand a phone call to a predetermined number. Possessing both should deter a common criminal looking for an easy score.

COVID-19 Concerns

I close this chapter with numerous privacy-related matters which have arisen during the COVID-19 crisis. Much of this book was written during the various stages of self-quarantine which was experienced by everyone throughout the world. While I selfishly benefited from the extra time which allowed early completion of this final draft, the pandemic introduced many new privacy concerns into all of our lives. This book will likely print before we see the end of these invasions, but I offer the following considerations for the next crisis.

Mobile Device Tracking

After most governments enacted rules which required people to stay at home unless travel was essential, we witnessed various levels of compliance. Some families practiced appropriate "social distancing" while others continued to attend large events. New cases of COVID-19 continued to emerge and many governments focused on technology as a possible solution. Many countries began tracking mobile devices in order to identify people who had possibly made contact with an infected person. The potential for abuse of this data is huge, so we should have an understanding of the technologies and threats.

Some countries relied on cellular connection details provided by mobile network providers. Cell phone tower logs can precisely identify the locations of devices (and people). This information can be used to detect large gatherings which violate local laws, or to identify devices which were within a few feet of a known infected person. Since most people purchase devices in their true names, it is easy to be identified as the owner of an account if you become a target. Some countries mandate that all device owners supply true information. In the U.S., we can easily mask our identity with prepaid plans, as previously explained.

Other countries have focused on application-based monitoring of COVID-19 infections. This requires effort by the end user while the previous cellular data monitoring is completely out of our control. I witnessed countries creating their own insecure apps which leaked potential sensitive data such as unique identifiers of hardware. In most scenarios, participation was voluntary. Some countries experienced a 20% adoption rate, but most needed at least 40% of the population to download the app in order for it to be effective. The typical goal with these apps is to identify people who may have come into contact with an infected person. If a participant is notified that he or she tested positive, this information can be reported through the app. The service then identifies devices which may have been in recent contact with the infected person and notifies them of the details. Typically, this occurs without disclosing any identities. However, apps created by government agencies usually are not very secure.

Finally, we have the execution of mobile device tracking by the U.S. government. Apple and Google partnered to create an infrastructure which could be used by third-party government

and private sector mobile applications. On the surface, this sounds incredibly invasive and undesired. You may be surprised to read that I welcome this partnership and execution. I will not pretend to understand all of the technical nuances presented by their teams, but I have great respect for their determination to never reveal any details which could be used to identify a person, device, network, or other unique identifier.

The product created by Apple and Google is not a tracking application ready for installation. It is simply a framework which can be used by other applications. It will be embedded into the iOS and Android operating systems. The benefit with this is that it removes the necessity for governments to apply privacy-respecting methods while creating a tracking service. The framework will never disclose a telephone number, MAC address, IP address, name, home address, email account, or anything else which would identify the device owner to any application connected to the free tracking service. It assigns everyone rotating unique identifiers which are never associated with hardware or personal details. This way, government apps can receive data about locations of infections without knowing any true identities.

The purpose this is to track movement of people and their proximity to others. When a person self-reports a COVID-19 infection through the app, it can notify others who may have been in contact with the infected person within the recent past. This happens behind the scenes without the ability to be abused. Have I drunk the Kool-Aid and installed the apps? No. However, I embrace any attempt to properly mask identities of individuals versus hastily created apps by government contractors with no respect for privacy. This method is the least of all evils. Further, I encourage these actions in effort to eliminate any future deaths from this disease. As of now, all participation is voluntary.

I am writing this in late April 2020. I do not know how the final product(s) appear as you read this. I suspect that devices will have an option to disable the tracking, but it will likely be enabled by default. Hopefully, COVID-19 is now a distant memory. If we are still in this pandemic, we could experience mandatory usage of these technologies. In that case, we should understand our privacy options. First, possessing an anonymous device prevents much of any potential abuse. If an app collects your true cellular number, there is little to glean from it if you executed the strategies previously explained. Next, consider the location of the device. If a mandatory tracking app is present, then anyone with access to the logs would know the location of the device every night. You can defeat this with my Faraday bag methods as previously explained. Turning the device "off" is not enough.

It is easy for a privacy enthusiast to label all device tracking as invasive and unacceptable. I can relate to these feelings, but I also want to stay alive and healthy. Safety always trumps privacy for me. Personally, I would only participate within these programs if I were located in an urban environment with high risk of delivering or receiving the disease, and I believed that my usage would be helpful. You should make your own decisions without influence from me.

Working and Schooling from Home

During the pandemic, we all experienced a new way of life. Working remotely from home became a normal day for most people. While many embraced the idea of working in sweat pants, most ignored the privacy invasions which accompanied the transition. Employers began demanding that employees install remote conference software on their own equipment, most of which possessed some level of snooping software, and "always-on" webcams became normal. Working from home can be viewed as a luxury by some and a curse by others. The techniques within the previous chapters should minimize much of your exposure, but we should be aware of some common scenarios.

- Remote conference software, such as Zoom, collects and stores a lot of personal information during use. Be sure to always use a VPN, provide anonymous contact details, cover your camera when possible, and never install the software on your primary computer. Consider a virtual machine or dual-boot computer with a Linux partition for work-related activities. An online search of "zoom privacy dangers" should provide more reasons to protect yourself than you desire to read.
- Many schools demand installation of specific software which allows teachers to monitor students at all times. In most scenarios, instructors can watch students through webcams while taking tests or participating in lectures. This is a slippery slope toward abuse of the captured video or an eventual data leak. I encourage everyone to cover their webcams at all times in these scenarios. If you receive pressure from the school to enable a camera, explain that it appears broken and it does not work on any other apps. Again, never install proprietary remote conferencing software on any primary personal computer.
- If you would like to hear a full hour of my thoughts on working and schooling from home, please listen to my podcast devoted to the topic (163-Working & Schooling from Home).

The Next Pandemic

My concerns as I write this are not about the current pandemic. Today, we still have some control over participation in contact tracing. By the time you read this, we may be under a full quarantine with mandatory access to our mobile devices. This would be quite difficult due to the privacy strategies available to us and the ability to simply conceal our devices in Faraday bags, but I never underestimate the capabilities of our government. I hope this book has provided the tools you need to take action which is appropriate for you, your family, and your desired level of privacy. Stay safe.

Chapter Fifteen

Physical Privacy & Security

In 2017, I co-authored a book about physical privacy and security considerations as part of the Complete Privacy & Security Desk Reference series. Both volumes of the series are now out of print and severely outdated, but there were many timeless strategies which can benefit us privacy enthusiasts. My attempt in this chapter is to briefly summarize the content of that book, which is not otherwise present in this edition, in a way which can be easily digested. I present a lot of content here, compressed into glossary-style text, which can be further researched if desired. My goal is to get you thinking about these considerations as you establish your new private life. Let's begin with protecting the physical privacy of your home.

Home Privacy

After you have spent so much effort moving into your new anonymous home, you should execute best practices in regard to your physical privacy. Titling your home to the name of a trust loses privacy protection if your trash contains personal mail, legal paperwork can be seen through windows, and your business cards are visible within your vehicle parked in the driveway. The following tactics should be considered at all times.

Park vehicles in garage: There are many opinions on this. Some believe leaving a vehicle outside the house may convince a would-be burglar to stay away since someone is likely home. However, you obtain a potential layer of security at the risk of losing privacy. An exposed vehicle displays a license plate which can be swept into various license plate recognition systems. It is also prone to vehicle burglary and displays a pattern of behavior. If the vehicle is always present, but then disappears one night, you may be inviting unwanted trouble while you are gone. My strong preference is to always park any vehicles in a garage without windows. This allows you to conceal vehicle identifiers, items being transported into and out of the vehicle, and creates an overall assumption that someone COULD be home.

Properly eliminate personal trash: In the United States, I am legally allowed to take possession of any trash in front of your home. I can "steal" all of the bags and analyze them later when convenient for me. In fact, I did this during numerous investigations when I was assigned to a drug task force in the late nineties. During one assignment, we were preparing to execute a search warrant at a home later in the week on an early Friday morning. A call to the local trash service confirmed that Thursday was "trash day". On Wednesday night, I drove

by the target location and observed several full trash bags within the designated pickup container. I grabbed them all and threw them in the trunk of my covert police vehicle. At the police department, I opened the bags and located paperwork confirming the main suspect resided at the home, receipts disclosing bulk purchases of drug-making supplies, and empty boxes of 9mm ammunition. While this evidence was circumstantial, the discarded ledger of completed and pending drug sales provided an interesting piece of testimony at the trial. You could have replicated my actions without any legal repercussions. While my clients are not hiding from drug-related search warrants, they do have concerns about stalkers, former lovers, and paparazzi. The following trash protocol is taught to anyone hiring me for a complete privacy reboot.

Isolate any trash or recycling which contains true identities. This can include mail brought into the home after delivery to a UPS store, unwanted documents, private photos, expired credit cards, or any other sensitive items. The rule is that there should never be any evidence of a person's true name or image in the trash or recycling containers. Often, I will remove any labels from shipments I have brought into my home which contain my name. I can recycle or discard the package material, but never the labels. Anything with a true name gets shredded into a cross-cut shredder. I currently use the AmazonBasics 6-Sheet High-Security Micro-Cut Paper and Credit Card Home Office Shredder (https://amzn.to/2SGjDQq). This device shreds paper into 5/32" by 15/32" pieces. While this is a strong start, some text can still be read within the pieces. Once weekly, I burn all shredded material in a designated container outside my home. The combination of these two techniques ensures evidence of my identity is not available in my trash.

Apply proper window treatments: The term "proper" is quite subjective here, but I offer my guidance to clients. Any windows displaying access to the garage should be covered at all times with a material which prevents any view. I prefer to apply frosted glass spray paint to the interior of all garage windows. This allows light to enter without exposing clear details and eliminates accidental movement of curtains or blinds which could allow viewing from the outside. I also try to identify the most common windows which will be viewed from a potential intruder. These are often the windows by the front and rear entry doors. Any window with easy access from a visitor should be covered with a curtain or blinds at all times. On occasion, walk the perimeter of your home in the way a potential intruder would investigate the premises. Identify any likely areas which could help determine that no one was home. Overall, you want privacy within living areas without the appearance of being a shut-in.

Eliminate personality from the exterior of the home: Before writing this chapter, I took a walk around my neighborhood. One home proudly displayed their child's high school football player number, which also identified the grade and school. I now know they have a high school senior named Tim who wears number 21. The house next to them displayed a large wood sign proclaiming the "Wilsons" to possess the home. Next to them, a neighbor possessed a sign

announcing their love for Scottish terriers and a doghouse identified as the home of "Max" and "Greta". One of my neighbors spray-painted his last name on his trash bin, and displays a notice in his yard about his wood-cutting services. All of these scenarios present enough vulnerabilities to initiate a believable social engineering attack. While highly unlikely, these details could be abused. I prefer my clients to display no signs of interest or names.

Eliminate personality from the interior of the home: This one may lose several readers. If you are in the need of extreme privacy, you should eliminate all items within your home which might disclose your name or immediate family members in view of guests. Consider a few examples.

Wall of Fame: Most of us, including myself many years ago, possess an office or other room which proudly displays our achievements. In 2010, my home office displayed numerous awards on the walls. When a Charter internet technician came to troubleshoot a dying modem, a quick glance at my wall launched an uncomfortable conversation about my work. I no longer display any awards and I encourage many clients to do the same.

Personalized Gifts: Many gifts include some type of personalization such as engraving or printing of a family name. If you have your true name engraved on a door knocker, but you have convinced your neighbors that your last name is something else, this could cause unwanted inquisition. If your wedding album, with a custom cover announcing the true names and date, is visible on the coffee table, it may generate questions which you do not want to answer. After a client with an extreme situation moves into a new anonymous home, I conduct a sweep, attempting to identify any items which may need to be hidden. This can also include trophies, crafts, blankets, and collectibles which are too revealing.

Family Keepsakes: This one is the most difficult. Many of us possess items which have been handed down through several generations. Old newspaper articles, historic photos, family recipe books, and anything else which displays a family name can be trouble. These items should be carefully stored out of public view. I have witnessed stalkers and ex-lovers sneak around a suspected new home of their target in order to confirm their suspicions. The presence of one item containing the victim's name could be enough to cause someone to take their obsessions further.

Home Security

While you may be anonymous, you are not invisible. Criminals may not care about your identity, but are happy to take advantage of a vulnerable home in order to steal your items. While not directly related to privacy, protecting your family and valuables from crimes of opportunity makes good sense. If you need an extreme privacy twist, consider the repercussions of allowing a crime to be committed at your home. A publicly-available police

report displaying your true name and address associated with a burglary can eliminate all privacy strategies in place up to this point. Therefore, it is in your best interest to protect your property from potential crimes and the need to involve law enforcement. I present several ideas, beginning inside the home followed by exterior considerations.

Keep your valuables out of sight: This one may seem fairly obvious, but most people ignore the recommendation. Jewelry boxes on top of dressers, rare firearms behind hanging glass frames, and expensive laptops on the kitchen counter are all enticing to a burglar. A home free of visible items which can be quickly sold or traded may be passed for a more lucrative option.

Hide small valuables in unique places: Most thieves want something small and valuable. Money, jewelry, prescription drugs, and collectibles can be removed from a home quickly, and hidden within pockets while walking down the road. Because of this, I recommend placing small valuables within items which would likely be ignored during a burglary. First, I want to discuss popular options which I think are awful ideas. I NEVER recommend the following.

- Hollow books: Many burglars will quickly analyze books on a shelf knowing that empty decoys are commonly used to store valuables. It does not take long to identify the overly thick book with little weight.
- Anything in bedroom: Most thieves go straight to the master bedroom in order to find valuable loot. This is likely the worst place to keep anything important.
- Freezer/Refrigerator: This has become one of the most popular places to hide valuables, and thieves have been paying attention. It is fairly easy to identify items in a freezer which appear out of place, and this should be avoided.

This leaves us with the following options which are more ideal.

- Trophies: Almost all trophies are hollow within the metallic-coated pieces. Unscrewing these and placing small valuables inside are likely to go undetected. Placing all of the trophies in a cardboard box in the garage will add even less interest. If you possessed my sporting ability growing up, you can buy your own trophies. I once visited a trophy store and asked if I could buy any defected items. I walked out with a box full of awards I could never earn at a cost of $10. These could be used to hide thousands of dollars.
- CD Player: I recall the days when a full-sized CD player within a stereo cabinet would be a prime target for a theft. Today, they are ignored and practically worthless. These oversized electronics consist mostly of open air. Removing a few screws on the back reveals an opportunity to store small and midsized valuables. Cassette decks are also great for this.

- Electrical outlet: As mentioned in a previous chapter, I prefer electrical outlets as hiding places for extremely small items. There is usually a small amount of space surrounding the outlet itself, and commonly a hollow wall nearby. I have never known a burglar to remove outlet faceplates to take a peek behind them.
- Novelty hiding devices: Be careful here, but you can find many common household devices which have been converted into empty hiding places on Amazon.

Present "Bait" to any burglars: Some physical security professionals laugh at me when I mention this, but I stand by my recommendation. I believe every home should have items which solely serve as bait to a would-be criminal. My favorite consideration is the small fire safe filled with heavy objects. I keep two Sentry fireproof boxes (https://amzn.to/2HPfyD2) in my home at all times. One is under my bed and the other is in my bedroom closet. Each are filled with four 5-pound plates taken from a set of old dumbbell exercise weights, a few rolls of pennies, and some loose change. They are locked with no keys in sight. When a burglar looks in these two places, which is extremely common for a thief, the safes will rattle and be heavy. Most will assume that a firearm or bullion is inside, and these two items will be top priority for taking.

This serves a few purposes. First, it wastes the energy and time of the burglar. Hauling out two 20-pound boxes is plausible, but not fun. Since most burglars do not bring a vehicle to the scene of the crime, he or she must carry this weight some distance. For bonus points, remove the plastic handles from the boxes to make carrying more difficult. If desired, a larger safe could be used with more weight. Next, this tactic may prevent a burglar from taking something more valuable. If he or she believes that a prize is already in hand, a second trip back may be viewed as an unnecessary risk. Finally, it serves as a clear indicator that a crime occurred. Many burglars enter and retreat undetected. They leave no sign of foul play until you discover the theft weeks later. This presents a good chance of avoiding capture. If you see that one of these boxes is missing, you know something happened.

Install a large safe: This is mandatory for any home in which I live. A large stand-up gun safe can hold a number of valuable items and can be made very difficult to move. They are never completely burglar-proof, but we can take actions to make them extremely difficult to compromise. First, only consider safes which have the option to be bolted into a floor. There are many installation variables, but the idea is that you bolt the safe from the interior into the flooring below. Ideally, this would be a concrete surface, but bolting into a wood floor is also an option. Proper safe installation is outside the scope of this book, but free information is plentiful online. While I demand my safe to be bolted into a floor within the interior of my home for easy access, I respect this is not always an option. Therefore, I offer a few suggestions for placement and weight which may burden a thief enough to move onto something else.

First, consider the location of the safe. I see many people place them in garages due to size and weight, but I do not approve of this. If it was easy to move into the garage, it will be just as easy to move out. I want to make it a struggle for the thief. I also want the safe within the home in case I need to access it quickly. If you keep your firearms in a safe due to the presence of children, you should be able to easily access them within your home in the case of an emergency, such as a home invasion.

For most clients, a large gun safe is placed in the basement. If the basement does not have an exterior door, this makes the safe especially difficult to remove. Carrying an empty 400-pound safe up the stairs is quite a challenge. Fill it with heavy items and you have a bigger problem. I have also placed safes behind false walls, but this usually requires carpentry abilities. Recently, I placed a safe within a closet in which the safe was wider than the closet doorway. Removing the trim and door allowed just enough room to squeeze it in. Securely replacing the trim and door created a scenario where the safe could not be slid out of the closet without repeating the process. Numerous three-inch screws through the solid wood trim into wall studs creates a frustrating experience for a burglar looking to escape quickly.

Many gun safes possess various gun racks in order to vertically store long guns. I usually remove these in order to possess an open box. On a few occasions, I have added custom shelving or premade short book cases from Ikea in order to take advantage of the space. My next goal is to make the safe as heavy as possible without exceeding an appropriate weight for the flooring. If within a basement with a concrete floor, I see no limitations. The heavier the safe, the less likely a burglar will try to remove it. I have used the following techniques on behalf of clients.

- Ammunition: I admit I am a bit of an ammunition hoarder. I am not a doomsday prepper, but I believe every gun owner should have more ammunition than they think they might need. My home safe contains over 100 pounds of ammunition which makes it extremely difficult to move.
- Bullion: I had a client who collected 10-ounce silver bullion bars. He believed this was a protection from a collapsing dollar, and had boxes of it. Lining the bottom of his safe with these bars added over 150 pounds of weight.
- Worthless Materials: If you simply want to add as much weight as possible to your safe, you can find numerous options at your local home improvement store. 50-pound bags of sand are less than $5.

If you possess a gun safe which only contains a few guns and a small amount of ammunition, two people can easily carry it out of your home. A 400-pound safe which contains 400 pounds of content creates a surprise for a criminal duo. While not impossible to remove, it will be very difficult and take some valuable time. Consider the desired content and location of your

safe before purchase. Once in place, consider storing any valuables within it and have some piece of mind while away from the house.

Utilize lamp timers: A home which is dark for 24 hours is probably empty. If it is dark for a few days, the residents are likely out of town. Placing an interior light on a timer can give the impression that someone is home. However, creating a pattern of specific times during which it is turned on and off can create an illusion of automation. Because of this, I prefer programmable timers which can be staggered. I currently recommend the BN-LINK 7 Day Digital Programmable Timer (https://amzn.to/2HLTgCc). It allows programming of two lamps at different times over multiple days. It also has a vacation mode which randomizes the times in which lamps are activated. Always test your settings before execution.

Consider fake television visuals: Many people leave lights on when they leave the home. This does not deter many desperate burglars. However, evidence of a television being watched is usually a sign that someone is home. A television left on constantly while you are away can be harmful to the device and a sign that this is a ruse to deter burglars. This is where I recommend a "Fake TV". This small device emits random lights which simulate the look of a television being used in a dark room. An example for less than $20 which I have used can be found at https://amzn.to/2vYalGx. Adding this product to a lamp timer can create a desired effect which can fool many into believing someone is home.

Consider audio applications: If you do not want to invest in timers and visual decoys, a simple AM radio can accomplish a lot. Pick a talk station, increase the volume enough in which it can be heard from every room, and leave. If a burglar enters, the audio may be enough to make him choose another home.

Install exterior lighting: Exterior motion lights are more affordable and brighter than ever before. If you do not have existing lights pre-wired and do not want to risk shocking yourself during installation, battery-powered and solar options are plentiful. Most burglars will move on if lights activate when they get near a home. This is a small sign that the homeowner takes security seriously and that there are likely additional security measures in place inside the home. This is a small layer of protection, but I see no reason to ignore this strategy.

Activate an alarm system: Alarms can be quite a deterrent. They can also be a huge privacy invasion, which I explain at the end of this section. First, let's focus on the benefits. If a burglar enters a home and triggers an audible alarm, he knows his time just became much more limited. He does not know if you subscribe to an alarm service which has just notified the police. A nosey neighbor may hear the audible alarm and choose to investigate. Either way, you are no longer an easy target and there is added pressure for him to leave quickly. Audible alarms wirelessly connected to sensors on doors and windows are plentiful. All have security weaknesses and are targeted toward the local amateur burglar. A sophisticated adversary will

know ways to defeat standard protection, but that threat is fairly rare, especially if you are not a heavily targeted individual.

I do not typically recommend any type of monitored alarm systems. I have many clients in Los Angeles who insist on this, and private security vehicles continuously respond to alarm activations day and night. My concern is due to false alarms which trigger a police response. Imagine you are in your anonymous home without any association to your true name. While working in the garage, your alarm malfunctions or is accidentally triggered. Your alarm company cannot reach you by phone to confirm everything is fine and dispatches the local police to check on things. An officer pulls up and determines you likely belong to the home. You will be asked to provide identification, and your name will forever be connected to your home within a police report. I simply cannot risk this for myself or my clients. I encourage them to stick with audible alarms which are not monitored by any outside agency.

Display signage of protection: Whether you possess a functioning alarm or simply want to convey that you do, alarm signage is an affordable and effective solution. Small alarm notification stickers strategically placed on doors and windows likely to be used for illegal entry may deter a random thief. Signs near the driveway and home announcing the use of an alarm system can also be helpful. Both Amazon and your local hardware store offer many options.

Replace locks, strike plates, and screws: This is another mandatory action taken on any home for myself or a client. Changing the locks is standard practice when moving into a new home. If renting, you may receive resistance from a landlord over this, but I believe the battle is worth the reward. If you can afford expensive locks such as those made by Medeco or Abloy, that is great. However, most of my clients simply do not want to spend over $200 on each door. Instead, I encourage them to look for the grade of the lock. Grade 1 is the highest rating a consumer lock can receive. Grade 1 deadbolts were once primarily limited to industrial buildings but are now abundant for residential use. However, the grade of the lock will become useless if you do not reinforce your strike plates.

A typical lock strike plate is a small piece of metal within the door frame. It is the "hole" in which the locking mechanism secures into the frame of the door. These are usually secured with two short screws and can be compromised easily with a swift kick to the door. Because of this, I highly recommend two strategies to better secure your exterior doors. First, replace the strike plate with a larger version requiring four screws (https://amzn.to/2VcIjS9). This may require you to modify the frame by chipping away room for the plate. Next, secure the plate with three-inch screws. This ensures that the plate is securely connected to the studs of the wall and make forced entry much more difficult.

Remove external keys: We have all seen a TV show or movie in which a person visits the home of a family member or friend and finds the front door to be locked. After a quick look

around, the person picks up a false rock or finds a hidden box which contains a backup key. Those days of innocence are over. Every burglar knows to look for a hidden key near the door and can spot a fake rock quicker than you or me. My stance is firm. Never place a backup key anywhere exterior to the home.

Install a fence for security (not privacy): Six-foot privacy fences are appealing. They prevent street traffic from seeing into your home and isolate you from the nosy neighbors sitting in their yards. However, this comes at a price. The same fence which prevents visibility into your home provides concealment for anyone committing crimes on your property. A steel security fence is ideal for those wanting to keep people off of their property while a solid privacy fence is appropriate for those wanting visual isolation. I am "on the fence" a bit on these. Identify your own priorities and proceed accordingly.

Secure utility boxes: Many homes possess a utility panel outside the home which is maintained by the power company. This could be on an exterior wall of the home or attached to a pole near the street. When open, it usually presents a single master switch which disconnects the power to the entire home. If you possess a box like this, please consider securing it with a high-security padlock. This will not prevent a prepared thief who brings bolt cutters, but it may thwart a burglar looking for any easy opportunity.

Modify patterns of behavior: The final recommendation to is to change things up. If you leave at the same time every morning and return at the same time every afternoon, you set a pattern of behavior which can be abused. While you may not be able to control departure times due to a rigid work schedule, there are other things you can do. Returning home during lunch on occasion may break up a routine being monitored by a criminal neighbor. Randomly leaving dirty work boots outside a front door may convince a passerby to move on. Even without a pet, a large dog food bowl and half-full water bowl near the door may be enough to convince a thief to move on. Combining this with a thick rope attached to the deck may create the appearance of a brutal guard dog within the home. Get creative.

Firearms

I am an advocate for gun ownership and concealed carry of firearms. I rarely leave my home without a firearm properly concealed and accessible. This is not a book about firearm safety, training, or concealment practices. Instead, I want to focus on a scenario which has presented problems to privacy enthusiasts. Every state in the country possesses unique laws about gun ownership, purchase, and carry. South Dakota has its own nuances.

If your domicile is South Dakota and you possess a PMB address on your driver's license, you can legally purchase a firearm while you are inside the state boundaries without a permit. If the seller possesses a Federal Firearms License (FFL), he or she will likely execute a

background check through the National Instant Criminal Background Check System (NICS). This usually results in a 48-hour hold on the sale. However, this is not required by state law and a private seller may not conduct a check. Overall, buying a gun within the state is fairly easy and straightforward. There is no official waiting period and weapons do not need to be registered with the state. While in the state, you can legally carry an unloaded handgun in the trunk or other closed compartment of a vehicle without any type of permit. Open carry is legal in South Dakota, which means you can carry a loaded weapon on your person without a permit, as long as it is visible to the public. Carrying a concealed weapon, especially in other states, is where it gets tricky.

South Dakota offers three levels of concealed carry license, and I will only focus on the "Enhanced" option which allows concealed carry in 37 additional states. The enhanced license requires fingerprinting, a federal background check, and a firearms safety course. It provides the most features in terms of reciprocities with other states. However, there is a catch.

South Dakota requires that the applicant has "physically resided in and is a resident of the county where the application is being made for at least thirty days immediately preceding the date of the application". By the letter of the law, you must be physically present within the state for a month before you apply. This could be a hotel or RV park with a physical address. I have spoken with numerous sheriff's deputies about this. Half insist on the physical presence while the other half stated that the PMB address is sufficient. If this is your scenario, I encourage you to do your own homework and contact the Sheriff's department within the county of your domicile. You can find complete current instructions for concealed carry permits on the South Dakota website at https://sdsos.gov/general-services/concealed-pistol-permits/default.aspx. Overall, I encourage potential South Dakota nomads to consider their firearm and concealed licensing needs when they conduct the rest of their transition to the state.

If you are not a South Dakota nomad, you are at the mercy of the laws of your state. I recommend visiting https://gunstocarry.com/ccw-reciprocity-map for more information. Being a nomad will always have potential negative implications in your legal ability to carry a firearm. I encourage you to keep advised of any changes in the laws of your state.

Chapter Sixteen

Advanced Private Digital Life

This chapter represents completely new material which was not present within the previous edition. While writing the previous chapters about digital communications and secure devices, I refrained from including some strategies which may be considered a bit too extreme for some readers. I worried that including the content within this chapter so early in the book may have discouraged some readers from continuing our journey toward complete privacy and digital security. Now that we are progressing toward the end of the book, I feel I can disclose some of my techniques for clients in extremely sensitive situations. The material presented here is all part of my own privacy strategy, but executed by only a few of my clients. Below is a summary of the ideas presented within this chapter.

Virtual Machines: One of the easiest ways to isolate sensitive computer usage is to prepare multiple virtual machines for specific tasks. This also provides an easy method to incorporate Linux into your daily digital life without committing to it as your only host OS. This section provides explicit tutorials for installation, execution, strategies, and troubleshooting.

Live USB Operating Systems: If virtual machines leave too much digital evidence on your personal device, consider USB operating systems. These devices allow full usage of a Linux operating system on practically any laptop without touching the internal hard drive. The TAILS system presented routes all internet traffic through Tor and saves no changes.

Advanced 2FA: The default services of a Yubikey, as previously mentioned, are likely sufficient for most readers. However, some of us like to push the boundaries. This section explains how to utilize multiple slots within the Yubikey hardware token and introduces OnlyKey, which provides 24 programmable slots for a complete credentialing solution.

DIY VOIP: This section presents a method of obtaining telephone numbers which can be used for communication within desktop and mobile clients. This is especially important for Android users and anyone wishing to leave the Google Voice ecosystem. When complete, you own the numbers supplied directly from the telecom provider, at a cost of $1 per month.

Alternative Android: Many readers may have concerns about Google and Apple collecting data from mobile devices. This section presents a custom Android system called LineageOS. By default, it never sends data to Google. However, it provides a complete system which supports any apps desired. If you do not want an iPhone, this is a great option.

Virtual Machines

Virtual machines (VMs) conduct emulation of a particular computer system. They are computer operating systems on top of computer operating systems. Most commonly, a software program is executed within an operating system, and individual operating systems can launch within that program. Each virtual machine is independent from the other and the host operating system. The environment of one virtual machine has no impact on any others. Quite simply, it is a way to have numerous computers within your single computer. When finished, you will have a "clean" environment with no contamination from other internet usage. You will be able to clone a master VM in minutes and will no longer need to worry about persistent viruses, tracking cookies, or other invasive tactics. We will use virtual machines in order to isolate our sensitive computer usage from the daily driver which gets bombarded with online tracking.

Before creating a virtual machine, you must possess virtual machine software. There are several free and paid programs which allow you to create and execute virtual machines. Premium options such as VMWare offer a free version, but it is extremely limited in function. However, VirtualBox is completely free and easy to operate. Most methods presented here for VirtualBox can be replicated on VMWare or any other virtualization software.

VirtualBox (virtualbox.org)

Volumes could be written about the features and abilities of VirtualBox. I will first explain how to install the application and then ways to configure a virtual machine. VirtualBox installation instructions can be found at virtualbox.org but are not usually straightforward. At the time of this writing, the following steps installed VirtualBox to my MacBook Pro.

- Navigate to virtualbox.org/wiki/Downloads.
- Click the appropriate link for your OS, such as "OS X Hosts" or "Windows Hosts".
- If required, select the highest version NOT including "Beta", such as "6.1.8".
- Download the appropriate "dmg" file for Mac or "exe" file for Windows.
- Download the Extension Pack for your version, such as "6.1.8.vbox-extpack".
- Install the dmg or exe file with all default settings.
- Double-click the Extension Pack and add it to VirtualBox.

The only requirement for VirtualBox to function is a computer that supports virtualization. Any modern Apple product will work without any modification. Most mid-range and high-end Windows computers made within the past five years should have no problem, but may require you to enable virtualization support in the BIOS (Basic Input / Output System) during startup. Netbooks, older machines, and cheap low-end computers will likely give you

problems. If you are in doubt about meeting this requirement, search for your model of computer followed by "virtualization" and you should find the answers. The rest of this section will assume that your computer meets this requirement.

Ubuntu Linux

This may be quite controversial to some Linux enthusiasts, but I recommend Ubuntu as an ideal Linux operating system for our private machine. While I use a Debian build for my own personal use due to the privacy and security of that operating system, Ubuntu is more appropriate for a wider audience. Debian can present complications when trying to display the dock or enable sudo features. If you are comfortable with Debian and insist on using it versus Ubuntu, go for it. For those who want an easier option, I explain the process using Ubuntu.

You may have heard of Ubuntu Linux. It is one of the most popular Linux distributions, and it is based on Debian as its backbone. Ubuntu is the product of a corporation called Canonical. Some criticize Ubuntu for including Amazon software in the default downloads, which provides affiliate funding to Ubuntu when you make an online purchase, but we will eliminate it once we are finished. The following could be replicated with other "flavors" of Linux if desired, with minimal differences within installation menus. As new versions of Ubuntu are released, you may see minor changes to the following tutorials. However, the general functions should remain the same. I urge readers to replicate these instructions with Ubuntu 20.04.

First, we need to download an ISO file containing the installation files for Ubuntu. The official website is very user-friendly, and can be reached at ubuntu.com/download/desktop. This presents a Long-Term Support (LTS) option, which is currently 20.04. Clicking the "Download" button should prompt you to download the ISO file required to install Ubuntu. This will be a large file with an extension of iso. During this writing, my file was titled "ubuntu-20.04-desktop-amd64.iso". This file behaves similarly to a physical CD which would install Windows or any other operating system. The 64-bit version should apply to most readers and their computers. If you know you need a 32-bit version for an older computer, you will find it in the Alternative Downloads section of the site. Save the file to your Desktop or anywhere else to which you have easy access. Expect an approximate file size of 2GB. Next, open VirtualBox and click on the button labeled "New". The following steps should create a new VM appropriate for our needs.

- Provide a name of "Privacy Master".
- Choose your desired location to save the machine on your host (I chose Documents).
- Select "Linux" as type, "Ubuntu 64-bit" as version, and click "Continue" (or "Next").
- In the Memory size window, move the slider to select 50% of your system memory.
- Click "Continue" and then "Create".

- Leave the hard disk file type as "VDI" and click "Continue" (or "Next").
- Select the default option of "Dynamically allocated" and click "Continue" or "Next".
- Choose the desired size of your virtual hard drive. If you have a large internal drive, 20GB should be sufficient. If you are limited, you may need to decrease that number.
- Click "Create".

Your VM has been created, but it will do nothing upon launch. We need to tell it to boot from the ISO file which we previously downloaded. Select your new machine in the menu to the left and complete the following steps.

- Click the "Settings" icon then the "Storage" icon.
- Click the CD icon which displays "Empty" in the left menu.
- Click the small blue circle to the far right in the "Optical Drive" option.
- Select "Choose Virtual Optical Disk File" and select the Ubuntu ISO downloaded.
- Click "OK" and then "Start" in the main menu.

Your Ubuntu installation process should now start within a new window. You should be booting to the ISO file previously downloaded, which is behaving as if you had placed an Ubuntu install CD into the virtual computer. This is your first virtual machine running on top of your host operating system. We can now finish the installation with the following steps within the VirtualBox window of your Ubuntu installation.

- Select "Install Ubuntu".
- Select your desired language and location then click "Continue".
- Select "Normal Installation", "Download Updates", and "Install third party…".
- Click "Continue".
- Select "Erase disk and install Ubuntu", then "Install Now", then "Continue".
- Choose your desired time zone and click "Continue".
- Enter a name, username, computer name, and password of your choosing.
- Allow Ubuntu to complete the installation, choose "Restart Now", and press Enter.
- If prompted, allow the installation media to be removed.

Your device should now boot to the login screen. In my example, it booted directly to the Ubuntu Desktop. The following will finish the default configuration.

- Click "Skip", then "Next", then "No", then "Next".
- Click "Next" then "Done" to remove the welcome screen.
- If prompted to install updates, click "Remind me later".

You now have a functioning virtual machine which contains the basic programs we need to use the internet. By default, it is using your host computer's internet connection, and taking advantage of your host's VPN if you have it connected. Technically, we could start using this machine right away, but the experience would get frustrating. We need to take some additional steps to configure the device for optimum usage. The first step should be to install VirtualBox's Guest Additions software. This will allow us to take advantage of better screen resolution and other conveniences. Conduct the following steps.

- In the VirtualBox Menu, select Devices > "Insert Guest Additions CD Image".
- Click "Run" when the dialogue box pops up and provide your password.
- Allow the process to complete and restart the VM.

You should now have VirtualBox Guest Additions installed. You can test this by resizing the screen. If you make the Ubuntu VM full screen, you should see the overall screen resolution change with it. If this appears to be functioning, you can right-click the CD icon on the desktop and choose "Eject". If not, double-click the CD icon and choose "Run Software" in the upper right corner to repeat the process. Next, we should make some modifications within the VirtualBox program in order to experience better functionality. Shut down the Ubuntu VM by clicking on the down arrow in the upper right and choosing the power button, followed by "Shut down". In VirtualBox, select your Ubuntu VM and click the "Settings" icon. Next, conduct the following steps.

- In the "General" icon, click on the "Advanced" tab.
- Change "Shared clipboard" and "Drag n' Drop" to "Bidirectional".
- In the "Display" icon, change the Video Memory to the maximum.
- Click "OK" to close the settings window and restart your Ubuntu VM.

You should now have a more robust display and copy and paste capabilities. This has improved a lot of function, and now it is time to personalize the machine. Personally, I do not like the default colors and wallpaper of Ubuntu, and prefer something more professional. I also want to modify many of the privacy settings for Ubuntu. I conducted the following on my new VM.

- Click the "nine dots" in the lower left to launch the Application Menu.
- Open Terminal and enter the following commands to make the background solid.
- gsettings set org.gnome.desktop.background picture-uri "
- gsettings set org.gnome.desktop.background primary-color 'rgb(66, 81, 100)'
- Close Terminal and open Settings from the Applications Menu.
- In the "Settings" menu, click "Notifications" and disable both options.

- Click the "Privacy" option, click "Screen Lock", and disable all options.
- Click "File History & Trash" then disable the option.
- Click "Diagnostics" then change to "Never".
- Click the back arrow, click "Power", and change "Blank Screen" to "Never".
- Click "Automatic Suspend" and disable the feature, then close all Settings windows.

These changes should create a more private and pleasing environment. This VM already possesses the latest version of Firefox, which is the browser I use most. However, I like to have the Tor Browser available to me, which was previously explained. The following command within Terminal installs the latest version.

- sudo apt install -y torbrowser-launcher

You should now have a Tor Browser option within the Applications Menu. Opening this should complete the installation. It is important to keep the software on this master VM updated. There are different ways to do this, but I will focus on the easiest way within the operating system applications. While we do this, it may be a good time to add some commonly used applications to our Dock. Conduct the following steps.

- Click the nine dots to launch the Applications Menu.
- Type "Terminal" into the search field.
- Right-click on the application and select "Add to Favorites".
- Type "Software" into the search field and right-click on "Software Updater".
- Select "Add to Favorites".
- Type "Tor" into the search field and right-click on "Tor Browser".
- Select "Add to Favorites".
- Press escape until all windows are gone.
- Launch the Software Updater icon from the Dock.
- Click "Install Now" and allow the updates to complete.

You now have Terminal, Tor Browser, and Software Updater in your Dock for easy access. You can also right-click on any undesired icons within the dock and easily remove them. Check for updates weekly and keep your master copy ready for usage. This brings us to a conversation about the term "Master". Ideally, you will keep a copy of this VM clean and free of any internet usage or contamination. There are two ways to achieve this, and both have unique benefits. First, let's discuss Snapshots.

Snapshots

A great feature of virtual machines is the use of Snapshots. These "frozen" moments in time allow you to revert to an original configuration or preserve an optimal setup. Most users install the virtual machine as previously detailed, and then immediately create a snapshot of the unused environment. When your virtual machine eventually becomes contaminated with remnants of other investigations, or you accidentally remove or break a feature, you can simply revert to the previously created snapshot and eliminate the need to ever reinstall. Consider how you might use snapshots, as detailed in the following pages.

Upon creation of a new Ubuntu virtual machine, apply all updates as previously mentioned. Completely shut down the machine and open the Snapshots option within your virtual machine software. Create a new snapshot and title it "Master". Use this machine for a single investigation, and export all evidence to an external USB device, such as a flash drive. You can then "restore" the Master snapshot, and it overwrites any changes made during the previous investigation. Upon reboot, all history and evidence is eliminated. This ensures that you never contaminate one virtual machine with another. When there are substantial updates available for Ubuntu, you can load the default configuration, and apply all updates. You can then shut the machine down completely and delete the Master snapshot, without saving it, and create a new snapshot titled Master. This new snapshot possesses all of the updates. If using this technique, I usually delete and create a new snapshot weekly. The use of snapshots is very similar between VirtualBox and VMWare, but let's take a look at the minor differences.

VirtualBox use of Snapshots

- Completely shut down the Virtual Machine.
- In the VirtualBox Menu, click on the Snapshots button in the upper right.
- Click on the blue camera icon to "take a snapshot".
- Create a name for the snapshot, such as "New Install", and click OK.

You can now use your virtual machine as normal. If you ever want to revert to the exact state of the machine that existed at the time of the snapshot, follow these instructions:

- Completely shut down the Virtual Machine.
- In the VirtualBox Menu, click on the Snapshots button in the upper right.
- Select the desired snapshot to apply.
- Click on the blue camera icon with arrow to "restore snapshot".
- Deny the option to save the current data, and click Restore.

Optionally, if you ever want to remove a snapshot, simply use the icon with a red X. This will remove data files to eliminate wasted space, but you cannot restore to that image once removed. It will not impact the current machine state. Many users remove old, redundant snapshots after creating newer clean machines.

VMWare Use of Snapshots

- Completely shut down the Virtual Machine.
- In the VMWare Menu, click on the Snapshots button in the upper right.
- Click on the camera icon to "take" a snapshot.
- Create a name for the snapshot, such as "New Install", and click "Take".

You can now use your virtual machine as normal. If you ever want to revert to the exact state of the machine that existed at the time of the snapshot, follow these instructions:

- Completely shut down the Virtual Machine.
- In the VMWare Menu, click on the Snapshots button in the upper right.
- Select the desired snapshot to apply, click the "restore" icon, and click "Restore".

Optionally, if you ever want to remove a snapshot, simply use the "delete" icon. Today, I rarely use snapshots, as I believe they are prone to user error. I much prefer Cloned machines. These require more disk space, but provide a greater level of usability between usage scenarios. Examples are explained in greater detail later.

VM Exports and Clones

If you ever want to preserve a specific state of Ubuntu, you can export an entire session. As stated previously, I prefer Clones over Snapshots. I create an exact replica of my master VM for every scenario, and never use Snapshots within these unique VMs. For clarity, consider my routine for online banking, which takes advantage of the "Clone" option within VirtualBox.

- Launch the Master VM weekly to apply updates or global changes, then close the VM.
- In the VirtualBox menu, right-click on the Master VM and select "Clone".
- Create a new name such as Banking.
- Click "Continue" (or "Next") then "Clone".

This creates an identical copy of the VM ready for my online banking. I have no worries of contaminating my master VM or any other copies. I now have a second virtual machine which I can launch when I want a secure operating system which can be used to connect to my bank

online. Since I never use this machine to surf the web, conduct searches on Google, or buy products on Amazon, there are virtually no trackers other than those issued by my bank.

Troubleshooting

I wish I could say that every reader will be able to easily build virtual machines on any computer. This is simply not the case. While most computers are capable of virtual machine usage, many demand slight modifications in order to allow virtualization. Let's take a look at the most common errors presented by VirtualBox upon launch of a VM.

VT-x is disabled: Any version of this error is the most common reason your VMs will not start. This indicates that the processor of your computer either does not support virtualization or the feature is not enabled. The fix for this varies by brand of machine and processor. Immediately after the computer is turned on, before the operating system starts, enter the BIOS of the machine. This is usually accomplished by pressing delete, F2, F10, or another designated key right away until a BIOS menu appears.

Once in the BIOS, you can navigate through the menu via keyboard. With many Intel processors, you can open the "Advanced" tab and set the "Virtualization (VT-x)" to "Enable". For AMD processors, open the "M.I.T." tab, "Advanced Frequency" Settings, "Advanced Core" settings, and then set the "SVM Mode" to "Enable". If none of these options appear, conduct an online search of the model of your computer followed by "virtualization" for instructions.

VT-x is not available: This is usually isolated to Windows 10 machines. Navigate to the Windows Control Panel and open "Programs and Features". Click "Turn Windows features on or off' and uncheck all "Hyper-V" features. Click "OK" and reboot. If the Hyper-V option is not enabled, enable Hyper-V, restart the computer, disable Hyper-V, and reboot again. Attempt to start your VM with these new settings.

This may seem backwards, but it makes sense. Previous versions of VirtualBox cannot run if you are using "Hyper-V" in Windows. Basically, both systems try to get exclusive access to the virtualization capabilities of the processor. Hyper-V within Windows receives the access first and impedes VirtualBox from the capabilities. The latest version of VirtualBox attempts to correct this. If the previous setting did not help, try to re-enable all of the Hyper-V options within Windows, reboot, and try to boot your VM again.

If you are still experiencing problems, read the troubleshooting chapter of the VirtualBox manual at virtualbox.org/manual/ch12.html. Expand any errors received and search the provided error codes to identify further solutions.

Virtual Machine Usage

Your master VM should only be used to install new software and apply updates. It should never be used for online browsing or research. I launch my master once a week, apply all updates, and close it. I can then use this master to create a clean and updated virtual machine within minutes. Next, I outline some of my uses for virtual machines.

Banking: I keep a VM designated for anything associated with financial transactions. This includes online bill pay, employee payroll, and investment accounts. This way, I know that the VM is free of any viruses or malicious applications. Since it is never used outside of banking, online tracking is minimal.

Shopping: I confess that I rely on Amazon for many things. I place an order at least once a week. When I do, I boot into my VM designated for online shopping. This VM is never used with any email, social network, or banking accounts. Furthermore, the entire VM is never associated to my true name. It is only used for ordering items with an alias. This way, I know that Amazon never learns my name or identifies any online browsing history.

Research: I conduct a lot of investigations. In my book Open Source Intelligence Techniques, 7th Edition, I explain how I rely on numerous VMs. Every time I need to research something or someone, I clone my master VM and open the clone. When finished, I either destroy the clone or export it for archiving. This way, each investigation possesses no contamination from other research.

Sensitive Consultations: When a client needs extreme privacy, I always communicate through a Linux VM which has never been used anywhere else. This is likely overkill, but I justify the paranoia. When communicating through Wire via text through this VM, I know there are no malicious programs, cookies, or other invasive software compromising the communication.

If you want to go the extra mile in achieving extreme privacy, I encourage you to understand virtual machine usage, and build VMs ready for cloning. At any given time, I have no fewer than five VMs ready for action. While most of my VMs are based on Linux, you can replicate these steps with a Windows machine. You will need installation media, such as a Microsoft Windows ISO file, and a valid license. Alternatively, you can download pre-built Windows VMs provided by Microsoft from https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/. These machines can only be used for 90 days, but re-importing the downloaded file resets the clock. Expect annoying licensing notices throughout usage, but these machines are completely legal.

Live USB Operating Systems

A live USB operating system allows you to boot most computers directly from a USB flash drive containing a full operating system which does not rely on any other software from the installed hard drive. They can either be "persistent" with capabilities of writing and storing changes or "static" which do not allow modifications between uses. For our purposes, we want an operating system which does not store any changes and boots without leaving any traces on the USB drive or the computer being used. TAILS is the perfect product for this.

TAILS, an acronym for The Amnesic Incognito Live System, is a security-focused Debian-based Linux distribution aimed at preserving privacy and anonymity. When booted, all incoming and outgoing connections are forced through the Tor network, which was explained earlier. The system is designed to leave no digital footprint.

In a perfect scenario, a USB drive is inserted into a computer which is turned off. When booted, the USB device is chosen and only software from the removable device is presented. You should see an entire operating system which "forgets" all of your activity when shut down. A VPN is not required since your traffic is going through Tor. It includes a web browser and productivity tools by default. Before explaining how to create your own TAILS USB device, consider some reasons why it could be vital to your own situation.

Contaminated Machines: If you only have access to a single community computer, you have no way of knowing the history of viruses, spyware, and malware which has infected it. TAILS bypasses the hard drive and prevents unnecessary risk.

Network Monitoring: TAILS allows people to use the Internet anonymously and circumvent censorship. This includes networks which block specific websites. Journalists abroad often rely on this product when safely reporting issues back to their home countries.

Tech-Savvy Snooping: This is the main reason I send TAILS USB drives to potential clients. Many victims being held against their will only have access to computers and devices which possess software allowing their captors to see everything they do. I have met victims who had remote monitoring apps on their phones and keyloggers on their laptops. TAILS eliminates threats from any invasive software installed in order to eavesdrop on someone. I never want a potential client to communicate with me about an abusive situation if there is a chance the abuser can see the conversation.

Now that you have an idea of the benefits of TAILS, let's create a bootable USB device. The following steps download the required software and "flash" it to a USB drive.

- Navigate to https://tails.boum.org/install/download.
- Click the "Download" option.
- Save the "img" file on your computer.
- If desired, verify the authenticity of the download with the optional extension.
- Navigate to https://www.balena.io/etcher.
- Download and install the program version appropriate for your OS.
- Insert a USB 3.0 or higher flash drive into your computer.
- Launch BalenaEtcher.
- Click "Select image".
- Select the TAILS img file previously downloaded.
- In BalenaEtcher, click "Select target".
- Carefully select the USB drive inserted (contents will be erased) and click "Continue".
- Click "Flash" to begin the process.

When complete, you now possess a TAILS live USB. Insert it into a computer and turn it on. If the computer boots to the internal operating system, such as Windows or Mac, the machine's BIOS needs to be told to boot from the USB. The moment you turn on the device, look for any text such as "Setup" or "Boot" options. Press the key which is displayed for this option, such as CMD, F1, F2, F10, F12, or Del. This should present a minimal menu which allows you to choose the USB device instead of the internal hard drive. TAILS should detect any ethernet or Wi-Fi hardware and allow you to connect to the internet through Tor. If you experience any issues, navigate to https://tails.boum.org/doc.

These steps could be replicated with other operating systems such as Ubuntu, Mint, and even Windows 10. While I encourage you to explore other Linux options, I never recommend Windows bootable drives. You simply cannot stop Microsoft from collecting data about your usage every time you boot the machine. If you have a need for a secondary Windows installation, I encourage you to create one as a virtual machine, as previously explained.

If desired, you could create a Linux boot USB with persistent storage. This would allow you to save data during usage instead of wiping out all changes during shutdown. I never recommend this unless you have a specific need for it. A big advantage of TAILS is the ability to remove all evidence when finished. Adding persistence is a slippery slope toward possessing sensitive data in an insecure format. If you desire an alternative Linux operating system which stores changes, consider a dual-boot laptop. This would allow you to choose from two or more operating systems upon boot. There are ample tutorials online which explain this process for various models of computers.

Advanced Hardware 2FA

Previously, I explained the usage of a hardware token as part of a Two-Factor Authentication (2FA) strategy, such as the Yubikey, in order to protect your online accounts. In that writing, I explained the benefits of U2F over traditional OTP, both of which are provided by the USB Yubikey device. In this section, we will take things to another level. First let's revisit the best practices for a Yubikey, and I will demonstrate with a new Fastmail account created specifically for this explanation.

After logging in to the account, I navigated to Settings > Password & Security > Two-Step Verification > Add Verification Device. This allowed me to choose to use an authenticator app (such as Authy), U2F through a hardware token, or OTP with an older Yubikey. Since U2F is the most secure option, I chose that. Fastmail walked me through the steps to activate my Yubikey for their service. Now, any time I log in to Fastmail, I am prompted to touch my flashing Yubikey in order to complete the process. This prevents remote access to my email, even with a known password. I replicated the process to associate this Yubikey with test Gmail and Twitter accounts. Both used U2F by default. My Yubikey is now required for all of these accounts. However, there are additional features available to us through the Yubikey.

Yubikeys possess two virtual "slots" which can store small amounts of data. These slots can be used to facilitate a One-Time Passcode (OTP), static password, challenge-response credential, or OATH credential. By default, the first slot is designated for OTP. Since I do not use any services which rely on OTP (because I always use U2F), I can modify both of these slots. For the first slot, I will add a static password. In order to do this, we must download the free Yubikey Manager application, available for Windows, Mac, and Linux, from their website at https://www.yubico.com/products/services-software/download/yubikey-manager. After installation and launch, I conducted the following steps.

- Click on "Applications" and then "OTP".
- Under "Short Touch (Slot One)", click "Delete" and confirm.
- Under "Short Touch (Slot One)", click "Configure".
- Select "Static Password" and click "Next".
- Click "Generate" and click "Finish".

Your Yubikey now possesses a long and secure password in the first virtual slot. Any time you touch the device, it will type in this static password into any active window. The password never changes. This is not any type of 2FA, it is merely a convenience. This static password could be used to strengthen account security, especially when associated with a desktop application. Consider the following examples, assuming that my static Yubikey password is RkDNTRggchNceYTknLBjDNiNrJrhcFvjbRCHrt (my actual test password).

Secure Messaging: When I open Wickr on my Desktop, I must provide a password. Since I insist on my passwords being lengthy and secure, I must either manually type in the credential or copy and paste one from my password manager (KeePassXC). Alternatively, I could make the password for Wickr RkDNTRggchNceYTknLBjDNiNrJrhcFvjbRCHrt and simply tap my Yubikey every time I need to log in. While convenient, this does pose some risk. If anyone possessed my Yubikey, the password could be entered without my input or any knowledge of the credential. Therefore, I always add unique characters before the password. As an example, my password for Wickr could be wickr!4RkDNTRggchNceYTknLBjDNiNrJrhcFvjbRCHrt. In other words, I could type wickr!4 and then tap the Yubikey. This would allow me to continue using this static password with other applications and services without replicating the exact same password everywhere. Overall, this is more convenience than security, but it can add password complexity in various scenarios. I would never recommend this for all of your online accounts. I bring up Wickr because it is an application which I open many times every day. In order to access my account, you would need to know my username, my added characters (wickr!4) and my long Yubikey static password. If you have an application which requires constant input throughout the day, this could be a useful strategy. Be sure to store your static password within your password manager in case you lose or break the Yubikey.

Operating Systems: I use many computers throughout a typical day. I have my primary Linux laptop, a MacBook Pro for production purposes, a media center, a firewall, and other various devices. Let's focus on my media server. There is nothing overly sensitive present, but I do insist on a strong password and an encrypted drive. When booting this computer, it boots to Ubuntu Linux and prompts for a password. I do not have a physical keyboard or mouse attached to this unit, and the monitor is my television. Since I leave my Yubikey attached to my primary keyring, it is always with me. I simply plug the Yubikey into the front USB slot of the media center, touch the Yubikey, and my lengthy password is entered. The computer finishes the boot process and launches Kodi, which allows me to stream all of my audio and video. I do not recommend this strategy for personal computers containing sensitive information. If someone stole your Yubikey and Laptop, he or she would have everything needed to log in. I only recommend this for household devices which are not extremely sensitive.

Encrypted Containers: As I mentioned previously, I possess a VeraCrypt container which contains my KeePassXC database. In order to open the container, I must know the password. Since I cannot open my password manager without first opening the container, I cannot store my container password inside KeePassXC. Therefore, I must remember the password to the VeraCrypt container. Assume my memorized password is VC!76T84R911. That might be easy for me to remember, but it is not very complex. It is not obviously a VeraCrypt password, but it could use more characters. I could make my password to VeraCrypt extremely strong by using VC!76T84R911RkDNTRggchNceYTknLBjDNiNrJrhcFvjbRCHrt. I would then type VC!76T84R911 into the VeraCrypt password field and then touch my Yubikey.

Now that I have explained some uses for static passwords stored within a Yubikey slot, let's consider a "challenge-response" option for our KeePassXC database. Currently, you may have a secure password memorized for your KeePassXC password manager. You may want to add a layer of security to that strategy. After all, your password manager likely stores access to all your accounts. Open the Yubikey Management application, and conduct the following.

- Click on "Applications" and then "OTP".
- Under "Long Touch (Slot Two)", click "Delete" and confirm.
- Under "Long Touch (Slot Two)", click "Configure".
- Select "Challenge-response" and click "Next".
- Click "Generate" or create your own randomly generated secret key.
- Enable "Require touch" option.
- Click "Finish".

The second slot of your Yubikey is now configured for a challenge and response. You can now enable this feature within your password manager. Launch KeePassXC and open your password database. To be safe, you may want to make a copy until you have tested your final project. I save a copy any time I make security changes to a database. Conduct the following.

- Click "Database" in the file menu and choose "Change Master Key".
- Click "Add additional protection".
- Click "Add Yubikey Challenge-response".
- Ensure the application detects the Yubikey and click "OK".
- When prompted, touch the flashing Yubikey.
- Close the database and application completely, then reopen KeePassXC.
- Input the password, select your Yubikey in the "Hardware Key" field, and click "OK".
- When prompted, touch your flashing Yubikey.

You have now added an additional layer of security to your password manager. Every time you log in to the database, you will be required to insert your Yubikey and touch it. If you prefer, you could make this second slot another static password instead of a challenge and response. If you choose this route, a short press of the Yubikey will type the first static password while a long press of two seconds will present the second static password. Personally, I prefer the challenge and response availability. Since Yubikey allows only two slots, we have reached maximum capacity for our device. However, this is where the **OnlyKey** (https://amzn.to/2CVUF7l) enters our race. This device applies the same benefits of the Yubikey, but provides 24 virtual slots.

OnlyKey

The OnlyKey device is similar in size to the standard USB Yubikey hardware token. I prefer the Yubikey Nano device for daily use, as they sit practically flush with either a USB-A or USB-C port. However, the OnlyKey is much more powerful, and is always on my key ring. This device requires the OnlyKey application on a computer in order to easily program a PIN and customize complete function, but can be used on any computer without the software after it is configured. Therefore, let's install the application and configure the device. A current online guide is always available at https://docs.crp.to/usersguide.html.

- Navigate to the above website and download the OnlyKey app for your OS.
- Install the app with default options.
- Launch the app and click the "Guided setup" button.
- When prompted, choose and enter a PIN to protect the first 12 slots.
- When prompted, choose and enter a different PIN to protect the second 12 slots.
- When prompted, if desired, enter a self-destruct PIN.

When complete, your OnlyKey is now ready for use. When you insert it into a USB slot, you must enter the PIN assigned to either bank one or bank two before it can be used. After you have unlocked the bank, you can use it as a U2F device right away. You would set it up the same as the previous instructions for the Yubikey. Pressing any button (1-6) confirms the response as a U2F device. The power of the OnlyKey is the 24 slots which can be programmed with URLs, usernames, and passwords. Figure 16.01 displays the OnlyKey application.

After you have inserted the OnlyKey, opened the OnlyKey app, and entered the PIN for either bank one or two, you are ready to customize a slot. I conducted the following on a new OnlyKey which contained no prior programming. This example allows me to navigate to Twitter, enter a username, enter a password, execute the login, and apply U2F as a second factor of authentication.

- Click the button for the desired slot, for example "1a".
- Enter "Twitter" as a label.
- Provide a URL of "https://twitter.com/".
- Enter a delay of "2".
- Enter the Twitter username.
- Enable "Tab after UserName".
- Enter the account password and confirm.
- Click "Set slot".

I can now open a new browser tab and tap the "1" button on the OnlyKey and the device will go to Twitter and log me in. If I had set up U2F on the account, the OnlyKey would blink in order for a second tap (after login) which would complete the 2FA login. I can repeat this process to store up to 12 logins for each bank. Each button (1-6) has two options. Option "a" requires a single short tap of the button while option "b" requires a touch and hold of two seconds. You can also choose to store only a password if desired. Before you configure your credentials for 24 sites, we should discuss any security risks from these actions.

The availability of all needed credentials within a single hardware device is enticing and convenient. It also can be reckless. If I steal your OnlyKey and know your PIN, I have everything I need to log in to any accounts represented on the device. This is a scary, even if rare, possibility. I do not use the OnlyKey this way. Instead, I rely on it to strengthen other passwords, similar to the options presented earlier. The following is a fictional example of my OnlyKey slots based on my real usage.

1: Entire password to media center login
2: Entire password to media center FTP
3: Last 20 characters of Wickr password
4: Last 20 characters of Wire password
5: Last 20 characters of Authy password
6: Last 20 characters of Notes password
7: Session app ID 1 (to send to contacts)
8: Session app ID 2 (to send to contacts)
9: Forum URL, user, and password
10: Twitter URL, user, password, & 2FA
11: GVoice URL, user, password, & 2FA
12: FireRTC URL, user, and password
13: Last 20 characters of MacBook login
14: Last 20 characters of Apple password
15: Last 20 characters of Linux login
16: Full credentials to Wi-Fi router
17: Password to unlock this book in Word
18: Password to unlock my OSINT book
19: Terminal command
20: Terminal command
21: GVoice URL, user, password, & 2FA
22: GVoice URL, user, password, & 2FA
23: GVoice URL, user, password, & 2FA
24: GVoice URL, user, password, & 2FA

I present these storage options to give some ideas for your own configuration. Often, I use the OnlyKey to easily generate complicated text. As an example, I use Session as a secure messaging option with clients. It relies on a randomly generated "Session ID" which is used in place of a username. I need to send this information to clients, usually via email. I could never remember this long string of random characters, but it is only a button press away. Some services which are used as "burner" accounts, such as Google Voice, are not vital to keep extra secure. Storing the URL, username, and password for these accounts allows me to quickly and easily log in to the service. If I am expecting an incoming Google Voice call, I can press one button and be ready to answer in seconds versus opening my VeraCrypt container, providing a password, opening KeePassXC, providing a password, copying the Google username, pasting into the website, copying the password, entering into the website, and executing the login. Hopefully you now see the benefits of an OnlyKey. Figure 16.01 displays the OnlyKey application which identifies my configuration for the first 12 slots.

Now that you have configured your OnlyKey device, you should make a backup of the data. If you lose the device, or need to reformat for any reason, you can replicate your hard work easily. Personally, I keep a clone of my OnlyKey in a safe place for emergency usage. The following steps generate a backup file which can be imported into any additional OnlyKey.

- Launch the OnlyKey app, insert the device, and enter your PIN for the first bank.
- Click "Setup" and then "Set Backup Passphrase or Key".
- Click "Save passphrase or key" and document it in your password manager.
- Click "Backup/Restore" and click within the text box.
- Hold the "1" button on the device for at least five seconds.
- Allow the backup text to populate the input box.
- Click "Save file" and store the backup file safely.
- Repeat for the second bank of slots.

There are many additional benefits of the OnlyKey, and I have only focused on the most common features. Unlike the Yubikey, OnlyKey requires you to unlock the device when inserted into a USB port. This prevents a stolen device from being used without your consent. If the wrong PIN is entered ten times, the device wipes itself as a precaution. The device is not a threat if stolen or seized. I encourage you to visit https://docs.crp.to/usersguide.html and explore other possibilities.

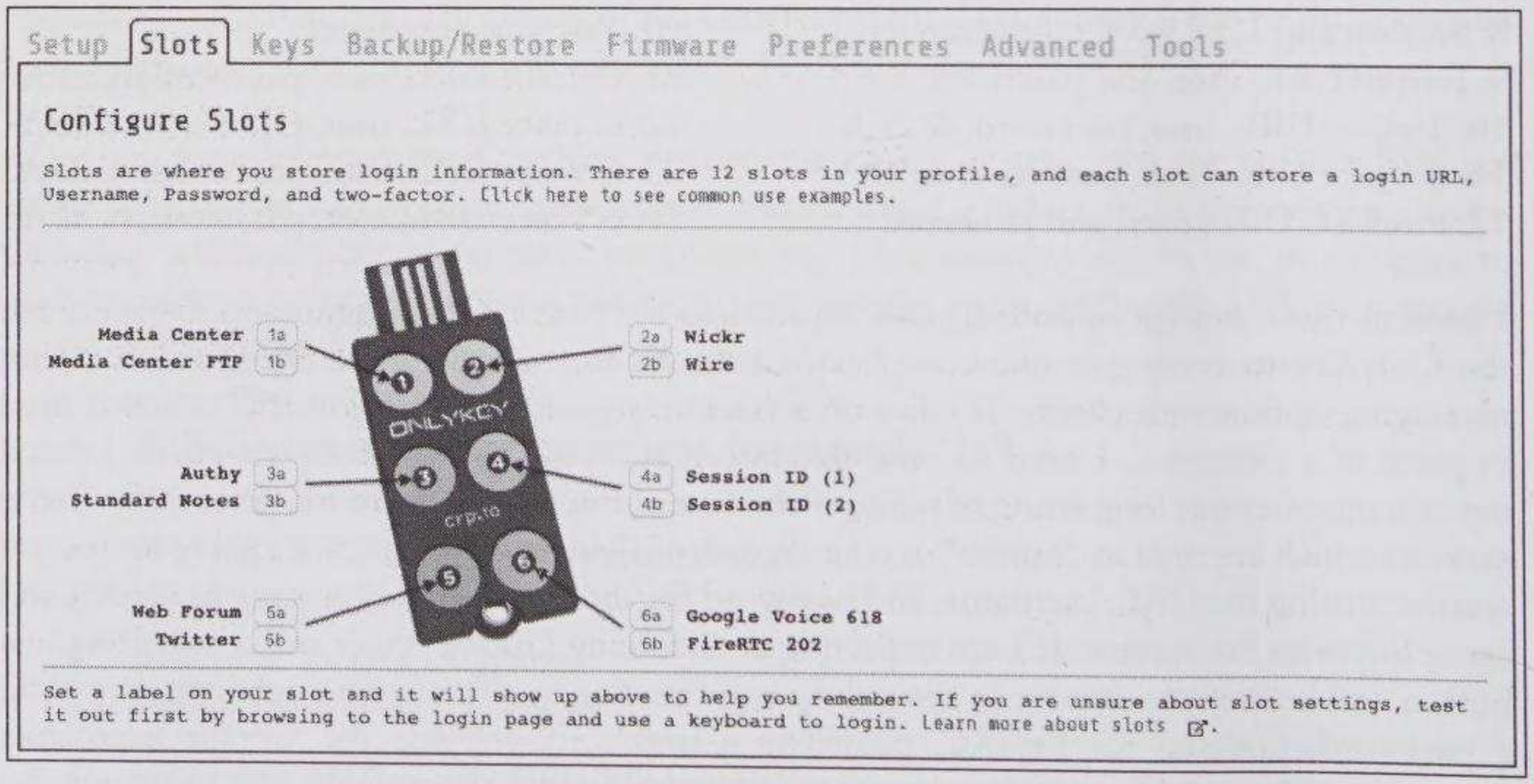

Setup
Slots
Keys
Backup/Restore
Firmware
Preferences
Advanced
Tools
Configure Slots
Slots are where you store login information. There are 12 slots in your profile, and each slot can store a login URL, Username, Password, and two-factor. Click here to see common use examples.
Media Center 1a
Media Center FTP 1b
2a Nickr
2b Wire
Authy 3a
Standard Notes 3b
4a Session ID (1)
4b Session ID (2)
Web Forum 5a
Twitter 5b
6a Google Voice 618
6b FireRTC 202
ONLYKEY
crp.to
Set a label on your slot and it will show up above to help you remember. If you are unsure about slot settings, test it out first by browsing to the login page and use a keyboard to login. Learn more about slots

Figure 16.01: The OnlyKey application displaying configuration.

DIY VOIP

Earlier in the book, I explained that I never use the cellular number assigned to my mobile device for any purpose. This is to avoid that number from becoming publicly associated with me which can then lead to SIM swapping attacks and non-stop tracking of my location. I mentioned two Voice Over Internet Protocol (VOIP) products including MySudo and Google Voice. At the time of this writing, desktop calling was not possible with MySudo. Google Voice works everywhere, including within desktop web browsers, but you give up a lot of privacy due to Google's invasive data collection. Neither are a perfect solution for everyone and both rely on upstream telephony providers. Most Google Voice numbers are provided by a service called Bandwidth LLC while every MySudo number is controlled by Twilio. What if we cut out the middle man?

My goal within the next few pages is to create our own VOIP product which allows us to make and receive telephone calls on any device we desire at minimal cost, all without subscriptions to a third-party service which facilitates the calls. Furthermore, the numbers will be in our control. We will not need to maintain access to a Google account in order to enjoy the benefits of VOIP calls. This section is very technical, but anyone can replicate the steps. As with any online service, any of these detailed steps can change without notice. It is probable that you will encounter slight variations of your details compared to my tutorial during your own configuration. Focus on the overall methods instead of exact instructions. The following explains every step I took in order to create my own VOIP solution with multiple numbers.

The first step is to create a new account at **https://www.twilio.com/referral/9FGpxr**. This is my referral link which gives you $15 of free testing credits and $10 of free full usage credits. I see absolutely nothing about you or your usage. You must provide a name, email address, and phone number to Twilio as part of this process. Twilio possesses strong fraud mechanisms in order to suspend accounts which seem suspicious. During the first tests of this strategy, my accounts were immediately suspended. I had provided a vague name, burner email address, and Google Voice number while connected to a VPN. This triggered the account suspension and I was asked to respond to a support email explaining how I would be using Twilio.

This began communication with two support personnel who were very helpful. While talking with customer support, I was advised that the VPN IP address was most likely the reason for the suspension. After providing a business name, "better" email, and explanation that I would be using the product for individual VOIP solutions, my account was reinstated. If you get caught within this dragnet, I encourage you to let them know you are following the protocol in this book to establish "VOIP through Linphone". I think you will find your account restrictions lifted within an hour. Twilio may push for a real phone number, but I have never provided anything besides a Google Voice number. My advice is to provide a unique name, non-burner email address, and Google Voice number during registration. If Twilio demands

a copy of government ID, push back. I was able to activate two accounts without ID after initial suspension. Overall, they just want paid users who do not abuse their networks.

I will now assume that you have a Twilio account created with a strong password using the previous link. The free credits allow us to test many features of the service, but a $20 deposit will be required before our account is fully usable. Clicking on the upper left "down arrow" should allow you to create a new project. Choose this and provide a name for it. I called mine "voipcaller". This will likely require you to confirm a telephone number to "prove you are human". Fortunately, they accept VOIP numbers here, and I provided an unused Google Voice number. After confirming the number, answer the questions presented about your desired usage. The answers here have no impact on your account. Once you have your new project created, you should see the new $15 test balance.

Within the Twilio Dashboard, click the option to "Get a Number" halfway down the page. Either accept the generated number or use the search feature to find a number within your desired area code. Click the "Buy" button once you have identified an appropriate number. This will deduct $1 from your balance. Next, we must set up our VOIP number for later use with a VOIP application with the following instructions.

- Click the "All Products and Services" icon in the upper left menu.
- Choose the "Programmable Voice" menu option.
- Click the "SIP Domains" option and click "Create New SIP Domain".
- Enter a unique word as the "Friendly" name (I chose "voipcaller").
- Enter a unique word as the "SIP URI" (I chose "voipcaller").
- Under "Voice Authentication", click the red plus next to "Credential List".
- Enter a "Friendly" name of your full telephone number, such as +12025551212.
- Enter a "Username" of your full telephone number, such as +12025551212.
- Enter a secure password and click "Create".
- Under SIP Registration, click the "Disabled" button to enable it.
- In the "Credentials List" dropdown, choose your previously made credential.
- Click "Save".

You now have a SIP domain and credentials created which allow you to associate your Twilio account with VOIP software. Typically, this is through a VOIP server which provides calls to hundreds of telephones. However, we are going to use this as a single number which will be accessed through an open-source program called **Linphone**. Navigate to the official Linphone website at https://www.linphone.org/ and download the desired application for your environment. I downloaded the macOS and iOS apps to my laptop and iPhone and then conducted the following configuration.

- If prompted upon launch, choose "Account Assistant".
- Click the "Use a SIP Account" option and enter the following data:
  Username: Your full telephone number, such as +12025551212.
  Display name: Your full telephone number, such as +12025551212.
  SIP Domain: Your full domain created previously including "us1" after "sip".
  Example: voipcaller.sip.us1.twilio.com
  Password: The password you created for the credential account previously.
  Transport: TCP

Click "OK" until you return to the main application. You can now click the upper left corner in order to select your new account, or choose between multiple accounts if you add more. You should see a green light next to the account if the connection from Linphone to Twilio is successful. We can now make our first test call.

- Confirm that your Twilio account is selected within the Linphone application.
- In the search field at the top, input any known telephone number.
- Click the "phone" button to initiate a call.

You should receive an automated message thanking you for using your demo account. This confirms that we can place calls to Twilio's servers, but we are far from unlimited usage to real numbers. Next, we must configure incoming and outgoing calls through Twilio with the following steps.

- Return to the Dashboard in the upper left menu.
- Click the "All Products and Services" icon in the upper left menu.
- Click "TwiML Bins" and select "Create a New TwiML Bin".
- Provide a "Friendly" name of "incomingvoice".
- Place the following text in the TwiML box:

```
<?xml version="1.0" encoding="UTF-8"?>
<Response>
<Dial answerOnBridge="true">
<Sip>
{{To}}@voipcaller.sip.us1.twilio.com
</Sip>
</Dial>
</Response>
```

- Replace "voipcaller" with your own SIP Domain name.
- Click "Create" and "Save".
- Click the "All Products and Services" icon in the upper left menu.

- Click the "Phone Numbers" menu and click your telephone number.
- Under "Voice & Fax", then "A Call Comes In", choose "TwiML Bin".
- Select "incomingvoice" in the drop-down menu and click "Save".
- Click the "All Products and Services" icon in the upper left menu.
- Click "TwiML Bins" and click the plus sign to create a new bin.
- Provide a "Friendly" name of "outgoingvoice".
- Place the following text in the TwiML box:

```
<?xml version="1.0" encoding="UTF-8"?>
<Response>
<Dial answerOnBridge="true" callerId="{{#e164}}
{{From}}{{/e164}}">{{#e164}}{{To}}{{/e164}}</Dial>
</Response>
```

- Click "Create" and "Save".
- Copy the generated "URL" into your clipboard.
- Click the "All Products and Services" icon in the upper left menu.
- Click "Programmable Voice" and click "SIP Domains".
- Select your domain.
- Paste the copied URL into the "Voice Configuration" "Request URL" field.
- Click "Save".

Please note that I have supplied all of this Twilio code at https://pastebin.com/F7S6ZgTH in order to allow easy copy and paste. We are now ready to attempt another test call. You still cannot call any real number, but you should be able to place a call to any "Verified" number. If you provided a Google Voice number during account creation, that number is automatically verified. If you did not, complete the following to add a verified number for testing.

- Click the "All Products and Services" icon in the upper left menu.
- Click the "Phone Numbers" option and click "Verified Caller IDs".
- Add a new number which can be accessed.
- Confirm whether you prefer a call or text and verify the call or text to add the number.

Return to your Linphone application and attempt a call to the number which you have verified with Twilio. For me, it was my Google Voice number. After a brief message about your trial account, the call should go through. If you can complete a test call to your own number, your configuration is complete. You are now restricted to only calling verified numbers. If you would like to remove this restriction and be able to make and receive calls to and from any number, you must "Upgrade" the account. The following steps should be conducted within the Twilio website portal.

- Return to the Dashboard in the upper left menu.
- Click the button for "Account Credentials" and "Add a Credit Card".
- Provide any Privacy.com, credit, debit, or registered prepaid card.
- Apply $20 to the account.

You should now have an unrestricted Twilio account which should be fully functional for voice calls. Please do not upgrade the account until you know your test calls are going through. You should also have a fully functional VOIP application which can facilitate calls. Linphone can be used to place a call at any time from any device. Replicate your Linphone settings on as many mobile and desktop environments as you desire. Furthermore, you can add as many numbers as you wish, which is explained later.

Incoming calls will "ring" your mobile device or desktop as long as the Linphone application is open and your status is "green". Before you create dozens of new numbers, let's discuss the costs. Each Twilio number withdraws $1.00 every month from your balance. If you followed these steps, you are funded for almost three years of usage of the initial phone number. Incoming and outgoing calls cost $0.004 per minute. During all of my testing for this tutorial so far, I spent $1.21. There are several huge benefits with this strategy, as outlined below.

- You can now make and receive telephone calls through practically any device. Windows, Mac, Linux, Android, and iOS are all supported through Linphone apps.
- You have more control over your number(s). You are not at the mercy of Google, and their data collection, in order to process calls.
- You can add as many numbers as desired as long as you have the funds to support them. I have five numbers through Twilio and I can access all of them through every device I own. My annual cost for this, including my usage, is about $70. Twilio does not know my real name and only possesses a ProtonMail address and Google Voice number in association to my account.
- You can port a number into Twilio. If you plan to cancel a cell phone or VOIP number, you can port it into Twilio and still have access through Linphone.
- This process works well with custom Android ROMs, such as LineageOS, as explained later in this chapter.
- You can call international numbers (at increased costs). Most VOIP providers such as Google, Twilio, and others restrict calling to nearby countries. You can enable any country in Twilio by navigating to Programmable Voice > Calls > Geo Permissions.

Please think of this VOIP strategy as being similar to landline service. Linphone has no embedded voicemail or SMS text message capabilities and is only for voice calls. If you desire the ability to receive SMS text messages associated with this new Twilio number, conduct the following steps, or consider a forwarding strategy explained in a moment.

- Click the "All Products and Services" icon in the upper left menu.
- Click the "TwiML Bins" option and click the red plus to add a new bin.
- Provide a name of "incomingsms".
- Insert "<Response></Response>" within the TwiML field and click "Save".
- Click the "All Products and Services" icon in the upper left menu.
- Click "Phone Numbers" and select your number.
- Under "Messaging", and "A Message Comes In", choose "TwiML Bin".
- Choose "incomingsms" in the field to the right and click "Save".

Any incoming text messages to this number can now be read in the "Programmable SMS" menu option in your Twilio account. If you would like to send a text message from your number, you can choose the "Learn & Build" option within the "Programmable SMS" menu. SMS text messages cannot be pushed to, or sent from, your Linphone application using this VOIP strategy. While it is possible to implement this feature, it requires hosting your own web server and exceeds the scope of this book. If you want to forward any incoming SMS text messages to another number, such as Google Voice or MySudo, replace "<Response></Response>" from this tutorial with the text below. Replace 2125551212 with any number which you want to receive the text messages intended for your new Twilio number.

```
<Response>
<Message to="+12125551212">{{From}}: {{Body}}</Message>
</Response>
```

Next, consider voicemail. Some may prefer to have no option to leave a voice message. The instructions up to this point will either ring your Linphone application for 30 seconds and then hang up, or simply terminate the call right away if Linphone is not open and connected. I prefer this for some numbers, as I do not want the caller to be able to record a message. However, we can enable voicemail, tell Twilio to record the message, save it to their servers, and email us a link of the recording. Conduct the following within the Twilio Dashboard.

- Click the "All Products and Services" icon in the upper left menu.
- Click "TwiML Bins" and select "incomingvoice".
- Replace the current text with the following:

```
<?xml version="1.0" encoding="UTF-8"?>
<Response>
<Dial answerOnBridge="true" timeout="30"
action="http://twimlets.com/voicemail?Email=your@emailhere.com">
<Sip>{{To}}@voipcaller.sip.us1.twilio.com</Sip>
</Dial>
</Response>
```

- Replace "your@emailhere.com" with your desired email address.
- Replace "voipcaller" with your own SIP Domain name.
- Click "Save" and test the service.

If your Linphone application is open and connected, an incoming call should ring for 30 seconds. If you do not pick up the call in that time, the voicemail system presents a generic greeting and allows the caller to record a message. If Linphone is closed or not connected to Twilio, the greeting is presented right away. If a caller leaves a voicemail, you will receive an email at the address provided which includes a link to hear the recorded mp3 file. This recording can also be accessed by navigating to "Programmable Voice" > "Recordings" in your Twilio Dashboard. Similar to Google Voice, you can delete the recorded file from this menu. This file is not secure or private. It is very similar to the way a traditional cellular provider or Google Voice would store voicemails available to your device.

If you would like Twilio to transcribe incoming voicemail messages and include the text spoken within your notification email, add "transcribe="true"" within the "incomingvoice" TwiML bin file. Mine appeared similar to the text below.

```
<?xml version="1.0" encoding="UTF-8"?>
<Response>
<Dial answerOnBridge="true" timeout="30" transcribe="true"
action="http://twimlets.com/voicemail?Email=your@emailhere.com">
<Sip>
{{To}}@voipcaller.sip.us1.twilio.com
</Sip>
</Dial>
</Response>
```

As a reminder, all of the Twilio code presented during this section can be copied and pasted online from **https://pastebin.com/F7S6ZgTH**. If everything is working well, you might consider adding more numbers to your strategy in order to have a selection for voice and text. Much like MySudo provides up to nine numbers within the app, we can add unlimited numbers which can be accessed through Linphone. Keep in mind that additional numbers will extract funds faster. I only recommend additional numbers if you understand the reasons you need them. I present the abbreviated steps here. Refer to the previous tutorials for further explanation.

- Click the "All Products and Services" icon in the upper left menu.
- Click "Phone Numbers" and click the red plus to buy a new number.
- Select a new number within your desired area code and purchase the number.

- Click the "All Products and Services" icon in the upper left menu.
- Choose the "Programmable Voice" menu option.
- Click the "SIP Domains" option.
- Click the red plus to create a new SIP domain.
- Enter a unique word as the "Friendly" name (I chose "voipcaller2").
- Enter a unique word as the "SIP URI" (I chose "voipcaller2").
- Under "Voice Authentication", click the red plus next to "Credential List".
- Enter a "Friendly" name of your new full telephone number, such as +12025551212.
- Enter a "Username" of your new full telephone number, such as +12025551212.
- Enter a secure password and click "Create".
- Under SIP Registration, click the "Disabled" button to enable it.
- In the "Credentials List", choose your previously made credential and click "Save".
- Launch Linphone and click the "Account Assistant".
- Click the "Use a SIP Account" option and enter the following data:
  Username: Your full telephone number, such as +12025551212.
  Display name: Your full telephone number, such as +12025551212.
  SIP Domain: Your full domain created previously including "us1" after "sip".
  Example: voipcaller2.sip.us1.twilio.com
  Password: The password you created for the credential account previously.
  Transport: TCP
- Confirm that your new Twilio account is selected within the Linphone application.
- In the search field at the top, input any known telephone number.
- Click the "phone" button to initiate a test call.
- Click the "All Products and Services" icon in the upper left Twilio menu.
- Click "TwiML Bins" and select "Create a New TwiML Bin".
- Provide a "Friendly" name of "incomingvoice2".
- Place the following text in the TwiML box:

```
<Response>
<Dial answerOnBridge="true" timeout="30"
action="http://twimlets.com/voicemail?Email=your@emailhere.com">
<Sip>
{{To}}@voipcaller2.sip.us1.twilio.com
</Sip>
</Dial>
</Response>
```

- Replace "voipcaller2" with your own SIP Domain name.
- Replace "your@emailhere.com" with your email address for voicemail.
- Click "Create".

- Click "Save".
- Click the "All Products and Services" icon in the upper left menu.
- Click the "Phone Numbers" menu and click your new telephone number.
- Under "Voice & Fax", then "A Call Comes In", choose "TwiML" Bin".
- Select "incomingvoice2" in the drop-down menu.
- Click "Save".
- Click the "All Products and Services" icon in the upper left menu.
- Click "TwiML Bins and click the plus sign to create a new bin.
- Provide a "Friendly" name of "outgoingvoice2".
- Place the following text in the TwiML box:

```
<?xml version="1.0" encoding="UTF-8"?>
<Response>
<Dial answerOnBridge="true" callerId="{{#e164}}
{{From}}{{/e164}}">{{#e164}}{{To}}{{/e164}}</Dial>
</Response>
```

- Click "Create" and "Save".
- Copy the generated "URL" into your clipboard.
- Click the "All Products and Services" icon in the upper left menu.
- Click "Programmable Voice" and click "SIP Domains".
- Select your new domain.
- Paste the copied URL into the "Voice Configuration" "Request URL" field.
- Click "Save".
- Click the "All Products and Services" icon in the upper left menu.
- Click the "TwiML Bins" option.
- Click the red plus to add a new bin.
- Provide a name of "incomingsms2".
- Insert "<Response></Response>" within the TwiML field.
- Click "Save".
- Click the "All Products and Services" icon in the upper left menu.
- Click "Phone Numbers" and select your new number.
- Under "Messaging", and "A Message Comes In", choose "TwiML Bin".
- Choose "incomingsms2" in the field to the right.
- Click "Save".
- Click "Save" again and test the service.

If desired, disable the "Request Inspector" logging feature within Twilio at "Programmable Voice" > "Settings" > "Request Inspector" > "Disabled" > "Save". This does not stop Twilio from storing VOIP call metadata, but it does eliminate a small layer of internal logging.

You can now choose between two different numbers within your Linphone application. Whichever is chosen allows outgoing calls to be completed from that number. Incoming calls to both numbers will ring the app and allow connection regardless of the chosen account. Incoming text messages will be stored at the Twilio Dashboard and voicemail will be transcribed and sent to your email address. You could replicate this process for an unlimited supply of numbers, as long as you have the funding to support them.

While configuring Twilio within the Linphone application during testing of this strategy, I encountered several devices which presented authentication errors during usage. These usually claim that the Twilio credentials supplied to Linphone have failed and the user is prompted to enter the correct password. Supplying the appropriate password fails. This appears to be an issue with Linphone. I have found that removing the SIP settings from Linphone under the settings menu, and adding the identical settings back to the application fixes this issue. I have no idea why this happens.

It is important to note that VOIP telephone calls and messages are not encrypted and we should expect no privacy. However, I have some isolation from my true identity. I use these numbers mostly for outgoing calls, similar to my previous instruction on MySudo, such as calls to businesses. This strategy is an affordable option which allows telephone calls without relying on your cellular carrier-provided number. It can also be used to isolate outgoing "junk" calls which are likely to abuse your number.

Hosting your own VOIP solution through Twilio eliminates the "middle-man". I trust MySudo and their business model, and appreciate the turn-key solution they offer without needing any VOIP programming knowledge. It is essential for my clients who want an easy option with full voice, text, and email support. However, they currently do not support calls from within desktop apps, which is important for my daily operations. This new strategy provides the missing services I desired for my own usage.

There are many "burner" style services which give you free calls from a browser, but can pose great privacy risk. These include FireRTC, PopTox, and Globfone. Similar premium apps such as Burner and Hushed can also pose similar dangers. Any time you allow a third-party service to facilitate your calls, you are also allowing them to intercept and see your data. All of these services rely on a VOIP provider such as Twilio, so I believe we should consider creating our own solutions and eliminate any additional companies which are unnecessary. During testing, I attempted to replicate these services with Bandwidth LLC and Voip.ms. I do not recommend either of these companies. Bandwidth refused my numerous requests for service and Voip.ms demanded unredacted copies of my driver's license before an account would be confirmed. While Twilio had their own roadblocks during account creation, they were the only VOIP service which actually provided me service. Anticipate fraud-related hurdles, but know that you can break through the temporary annoyances.

Alternative Android Operating Systems

Previously, I stated that I carry an iPhone for daily use, and that practically all of my clients rely solely on iPhones for mobile communication. I stand by that comment, but also want to acknowledge that Android can be made more private with some effort. When done properly, many Android phones can be configured so they never "call home" to Google. For some, this can be a better privacy strategy than a stock Android or iPhone device because you have more control over your privacy. However, this comes at a cost. The instructions for replacing the stock Android operating system can be daunting. You will need to feel comfortable with modifying your device in a way which could be irreversible. If mistakes are made, you could "brick" the device, which could make it unusable in any way. However, if you possess an old Android device which is no longer used, those risks become minimal.

In the rare scenarios where a client wants to stay with Android, I always recommend **LineageOS**. It is a free and open-source operating system for smartphones and tablet computers based on the Android mobile platform. It is the successor to CyanogenMod, from which it was created when Cyanogen announced it was discontinuing development and shut down their infrastructure. The main benefit of LineageOS is that it is "Google-free". That statement is a little misleading since it relies on the Android operating system, but a default installation includes no Google applications which attempt to connect to Google servers. This will present some challenges, but also give us a very private device without the need to disable invasive features.

Some tech-savvy readers will scoff at using LineageOS if they believe options such as GrapheneOS are better because they have secure boot features which help eliminate physical intrusions into the device's firmware. While this is true, the number of devices supported are much fewer than LineageOS. If you possess a modern device which is supported by GrapheneOS, you may choose to research that option and replicate some of these steps toward your own custom installation. Since LineageOS is more stable, and supported by many more devices, I will focus this section on that environment.

The demonstrations within the following pages were conducted on a Google Pixel phone which I retired in 2017. It is an older device (2016), but still works quite well with LineageOS. Navigate to https://download.lineageos.org and look through the brand menu on the left. Choose the brand of your own Android device and click it to see the various models which are supported. It is vital to choose the exact hardware version. If your device is not listed, then you should not proceed. Regardless, there is always a chance of damaging your device through this process. Proceed at your own risk. I have never ruined a device during the past decade of re-flashing phones, but the possibility exists. Some of the aging devices supported can be found at your local cell phone store for less than $50. At the time of this writing, an original Google Pixel was $65 on Swappa.com.

Phase One: Reset Your Device and Enable USB Debugging

The first optional step is to completely wipe out your device and reset the operating system to the version which was present during purchase. This removes any software, customizations, and updates. It provides a clean environment and allows us to "start over". However, this may also require you to enter the previously connected Google account in order to verify authorized access. Many purists believe resetting the device is a necessary step in order to ensure you have eliminated any previous contamination. **Since we will be wiping the device completely when we install LineageOS, I typically skip this first step**. However, you may find it justified. Every device will have different requirements to complete a "hard reset", but the corresponding LineageOS device page should assist. For my Pixel, I performed the following. Details for your device may vary.

- Open the Settings app and tap "System" > "Advanced" > "Reset options".
- Tap "Erase all data (factory reset)" > "Reset phone".
- Tap "Erase everything".
- Reboot the device and proceed to the home screen.

If prompted, attempt to bypass any configuration options. You should not need to connect Wi-Fi at this point and a Google account should be unnecessary. Some screens may require input such as selection of language. If prompted to participate in location gathering, usage analytics, or any other Google "features", decline everything. None of this matters much, since we will be wiping everything out and starting over, but it is good practice.

Next, we need to enable USB debugging. Every version of Android has unique instructions for this, all of which can easily be found online. With my device, I conducted the following.

- Open the Settings app and tap "About phone" then tap "Build number" 7 times.
- Tap the back icon to return to the Settings app.
- Tap "System" > "Advanced" > "Developer options" or simply "Developer options".
- Enable the "Developer options" switch.
- Enable "USB debugging".
- If prompted with "Allow USB debugging?", tap OK to confirm.

Your device should now allow you to connect it to a computer and send commands from a desktop operating system directly to it. This is vital for the remaining phases. Next, we must configure our computer in order to facilitate this connection. There is simply no reliable way to install LineageOS using only a mobile device. We must configure a desktop operating system for use with an application called ADB.

Phase Two: Install and Configure ADB

The Android Debug Bridge (ADB) is a development tool that facilitates communication between an Android device and a personal computer via USB cable. This requires you to install Terminal (or Command Prompt) software to a computer and configure the operating system to see the application. There is no easy way to do this which will function reliably. Instead, we must download the software and modify existing files within the operating system throughout several steps. The procedure for this varies by operating system. Since most readers possess Windows 10, and anyone else can create a Windows virtual machine using the previous tutorials, I will only present Windows instructions here. Details for Windows, Linux, and Mac are available online at https://wiki.lineageos.org/adb_fastboot_guide.html.

- From within a Windows 10 computer or VM, navigate your browser to the address of https://dl.google.com/android/repository/platform-tools-latest-windows.zip and download the file to your Windows Desktop.
- Double-click this file and drag-and-drop the "platform tools" folder to your Desktop.
- Rename this new folder to "adb".
- Open the Start menu, and type "advanced system settings".
- Select "View advanced system settings".
- Click on the "Advanced" tab.
- Open the "Environment Variables" window.
- Select the Path variable under "System Variables" and click the "Edit" button.
- Click the "Edit Text" button.
- Append ";%USERPROFILE%\Desktop\adb" to the end of the existing definition.
- Click OK three times, once for each window.
- Navigate to https://adb.clockworkmod.com/ and click "Download".
- Double-click the downloaded file and allow the program to be installed.
- Connect your device to your computer or VM via USB cable.
- If using a virtual machine, choose to connect the device to the virtual machine.
- If prompted on the device, select "always" allow the connection.
- Reboot the computer or VM.
- Open a Command Prompt, type "cd Desktop\adb", and press enter/return.
- Type "adb devices" and press enter/return.

Hopefully, you see a result similar to "List of devices attached: 138uuhg device". If so, you are ready to proceed. If you receive any errors, unplug the device and plug back in, repeating authorization. Many things can go wrong here, and I can never anticipate every issue. Fortunately, there are thousands of support sites a Google search away. Your device must be recognized before you can proceed.

Phase Three: Unlock the Bootloader

The storage on an Android smartphone is similar to a hard drive made up of several partitions. One of those partitions holds the Android system files, another holds all the app data you accumulate, and others are hidden for stable functionality. The bootloader is a security checkpoint and manager for all of those partitions. Every computer has one, and it tells the hardware where to look and how to get running when you boot the device. On Android devices, the bootloader checks a few things to make sure the software you are trying to use is genuine. Custom operating systems would not pass verification checks upon boot. This is why we need to unlock the bootloader. Every device possesses unique steps to do this. Some devices require you to obtain an unlock code from the manufacturer. The following applied to the Pixel.

- Open the Settings app, enter "Developer options", and enable "OEM unlock".
- Connect the device to your computer via USB cable.
- Ensure it is detected by Windows.
- If connecting to a virtual machine, you may need to choose the appropriate VM.
- Open Command Prompt and enter the command "cd Desktop\adb".
- Enter the command "adb devices" and ensure the device is recognized.
- Enter the command "adb reboot bootloader" and the device should reboot.
- Verify the device is still recognized by typing "fastboot devices".
- Enter the command "fastboot flashing unlock".

The device should reboot on its own. If it does not, force a manual reboot by holding the power button to shut down and press it again to restart. Since the device resets completely, you will need to re-enable USB debugging to continue. The following instructions are replicated for your convenience.

- Open the Settings app and tap "About phone" then tap "Build number" 7 times.
- Tap the back icon to return to the Settings app.
- Tap "System" > "Advanced" > "Developer options".
- Enable the "Developer options" switch.
- Enable "USB debugging".
- If prompted with "Allow USB debugging?", tap OK to confirm.

Hopefully, your device is now ready for new software and your computer is ready to deliver it. You must be able to connect your device to your computer, execute commands through ADB, and verify that ADB can recognize the device in order to proceed. Without success of these steps, the following tutorials will not function.

Phase Four: Install TWRP and Download Custom Recovery

Before we can install LineageOS, we need to set up a "recovery image". This allows us to boot to a custom menu which provides an easy installation option from the device itself. First, you must identify the correct image designated specifically for your device. You should start at the **TWRP** website at https://twrp.me/Devices. Select the make and model of your device and replicate the following instructions.

- Under "Download Links" click the closest location.
- Download the most recent file ending in ".img".
- Rename the file to "1.img" and move it to the adb folder on your Desktop.
- Connect the device to your computer.
- Open Command Prompt and type "cd Desktop\adb".
- Enter the command "adb devices" and ensure the device is recognized.
- Enter the command "adb reboot bootloader" and the device should reboot.
- Verify the device is still recognized by typing "fastboot devices".
- Enter the command "fastboot set_active a".
- Enter the command "fastboot flash boot_a 1.img".
- Enter the command "fastboot boot 1.img".

Note that every device possesses unique steps for this phase. The LineageOS Wiki page should present the appropriate steps for your hardware. When this phase is complete, the device should reboot into the new TWRP menu. If this fails, you can manually enter the TWRP menu by holding the pattern of buttons which loads the recovery menu for your device. For mine, I can hold the "Volume Down" and "Power" buttons at the same time while the device is off to enter the recovery menu.

There are many things which may go wrong for you. If any step is skipped due to an error, the remaining instructions will probably fail. It is very likely that you will need to research your own LineageOS installation problems. Aside from Googling your specific issues, the information available at https://lineageos.org should be very helpful. There are also numerous videos online which demonstrate the installation, possibly some specifically for your device.

Please remember that you may need to take extra measures to ensure the device connection to the computer if you are using a virtual machine. During the process of writing this section, I used a Windows 10 VM on my MacBook Pro. Each time the device would reboot, I had to notify my host operating system that I desired the device to connect to the VM. This can add additional frustration. However, possessing a virtual machine which is prepared for installation and updating of LineageOS can be very beneficial.

Phase Five: Install LineageOS

Surprisingly, this is the easiest part of the tutorial. We will now install LineageOS onto the device with the following instructions.

- Revisit https://download.lineageos.org/ and select your device from the left menu.
- Download the most recent "File" into the adb folder on your Desktop.
- Rename the file ending in ".zip" to "1.zip".
- While in the TWRP menu, tap "Wipe" then "Format Data".
- Return to the previous menu and tap "Advanced Wipe".
- Select the "System" partition and then "Swipe to Wipe".
- Return to the main menu.
- Select "Advanced", "ADB Sideload", then "Swipe to begin sideload".
- Return to the Command Prompt window from the previous phase.
- Enter the command "adb sideload 1.zip".
- Enter the command "adb reboot".

If all went well, your phone is now boot into LineageOS. There are no Google services installed, nor do we want any. I must confess that I ran into multiple problems during my own installations and various devices while testing for this book. I did not mention them here because they were likely unique to my setup. If you decide to create your own Google-free Android phone, expect complications. However, the end result is fantastic.

I now have an Android device that does not share any information with Google (or Apple). This is my go-to device when I need to use Haven (the surveillance application mentioned in previous chapters) when I am on the road. If you desire an affordable low-power LineageOS device, I recommend the Motorola Moto Z, Google Pixel, or Google Pixel XL. Each can be purchased used for under $80 online at swappa.com. If you plan to use your LineageOS device as a full-time mobile phone, consider the OnePlus 6T, available for $349. Regardless of your mobile device choice, make sure it is officially supported on the main LineageOS downloads page.

Overall, the installation process will vary greatly for every brand of mobile phone. I present the previous instructions in order for you to become more familiar with this process. Expect problems, errors, and frustration if you dive into this world. However, also expect a smooth Android device with a great level of privacy. Always refer to the official LineageOS website for the latest tutorials and downloads at https://lineageos.org.

Phase Six: Configuration of LineageOS

Your device is fairly private and secure, but there is always room for improvement. There are no Google services, and Google is not receiving any data about your usage. If you have configured F-Droid, as explained in a moment, you have access to plenty of apps which can be installed. However, I encourage you to follow the details presented within previous chapters and only install necessary software. Next, let's tighten some privacy and security settings. Consider the following modifications.

- Swipe up from the bottom of the screen to produce the applications menu.
- Open the Settings application and tap "Security" then "Screen Lock".
- Tap "PIN" and set a desired secure PIN.
- Return to the "Security" menu and tap "Encryption & Credentials".
- Tap "Encrypt Phone" twice and allow the process to complete.
- Return to the Settings menu.
- Tap "Location" and disable completely until needed.
- Return to the Settings menu.
- Tap "Privacy" then "Trust".
- If desired, disable "Security Alerts" in order to avoid daily notifications of status.

You now possess a mobile device which is more private and secure than any stock unit which could be purchased from a retailer. Unlike a traditional iOS or Android phone, a user account is not required in order to use the device. If ever prompted to add a Google account, avoid or "skip" the option. This way, there is no single Google or Apple account which can be tracked, archived, and abused. Again, by default, LineageOS transmits no data to Google. Eliminating these privacy threats provides great benefits.

The installation effort can seem overwhelming, but is usually only a one-time event. If you ever want to update your operating system, you can simply repeat Phase Five and apply a newly-downloaded LineageOS installation file. You will notice that the operating system is updated on the website often, sometimes daily. I typically update my software monthly. The update should not impact your installed applications, but the customizations within your settings menu may change.

This section may seem a bit unfair. Choosing any other device besides a Pixel will almost guarantee slight modifications to this tutorial. Furthermore, a Pixel is far from the best device for this usage. By the time you read this, LineageOS may have made changes which impact these lessons. My goal here is to simply encourage advanced users to consider a LineageOS device. These few pages can never replace the wealth of information available online.

Phase Seven: Installation of Apps & Device Backup

As mentioned previously, your new LineageOS device does not possess any stock Google applications. Since you have no way to install software from the Google Play store, I recommend installing **F-Droid** from within the device itself. Simply navigate to the official website at https://f-droid.org and choose the "Download F-Droid" button to install the apk file. This is a limited version of an app store which allows you to download Android apps without using Google's services. This provides access to many apps, but not everything. If you want to install an app which is not present within F-Droid, such as Session, Wickr, Wire, or Signal, you will need a third-party option.

Along with F-Droid, I recommend the application Aurora Store (AuroraOSS). Aurora Store is an unofficial client to Google's Play Store. You can search, download, and update apps. You can also spoof your device information, language, and region to gain access to the apps which are restricted in your country. Aurora Store does not require Google's proprietary framework. With Aurora Store, you can install most of the apps mentioned previously. If you ever find an application missing from both F-Droid and Aurora Store, search for the APK file for it and download it to the device. Aurora Store can be installed from https://auroraoss.com/ or through F-Droid. During installation, be sure to choose "Anonymous" mode, which prevents Google account requirement.

While your desired apps should install without issues, everyday function may be a problem. Since LineageOS does not contain any Google apps, you are likely missing some core Google software which provides services such as push notifications and mapping. You can usually still open apps and "fetch" data such as pending email or text messages at any time, but you might be missing instant notifications. With some apps, synching of content might simply be delayed.

Most private messaging apps, such as Wire, should deliver messages instantly through their own platform without the need for Google's push service. Traditional email applications, such as Fastmail, may only fetch the data when the app is opened. This may be a desired feature to some. A true Google-free experience without constant incoming notifications is a nice change. Personally, I prefer to intentionally fetch desired content when needed in order to keep Google out of my business. However, some clients demand the full scope of Android's features, such as Maps. In these rare situations, I hesitantly recommend a third-party software suite called **microG** (microg.org). microG allows Android apps to access the same application programming interfaces (APIs) which are traditionally provided by Google Play Services. I decided not to explain the process of installing microG in this book. If you want these Google core services, there is little reason to go to the extreme with LineageOS. I believe the biggest benefit of LineageOS is that Google is not present or calling "home" to share data of our usage. Adding services such as microG defeats the purpose of all of our hard work configuring these settings.

Backup & Restore

Once you have your device configured as desired, you should consider creating a backup. If your device should become corrupt or stop functioning appropriately, you would otherwise need to start over with a new installation. Fortunately, TWRP allows for easy backup.

- Boot into recovery mode in the same way as when you installed TWRP.
- Click the "Backup" button.
- Select all available data options.
- Click "Select Storage" and choose the SD card within the device.
- If TWRP asks if you want to root your phone, choose "Do Not Install".
- Slide the "Swipe to Backup" option to begin the process.

As long as you had enough free space on the SD card, you should now possess a valid backup of all software on your device. If you should ever want to return to this state, restore it with the following steps.

- Boot into recovery mode in the same way as when you installed TWRP.
- Click the "Restore" button.
- Select all available data options.
- Slide the "Swipe to Restore" option to begin the process.

At the end of this writing, I possessed a primary LineageOS device which made no calls "home" to Google. I recycled old hardware, including a $40 Moto G3, into lightning fast Android devices. I could apply updates to the OS as often as desired. All apps were functioning and updating properly including ProtonMail, ProtonVPN, Linphone, Wickr, Wire, Session, Signal, Authy, Mint Mobile, Standard Notes, Firefox Focus, and KeePass2Android. I never installed microG and never provided a Google account.

While my experience with LineageOS was fun, my daily-driver Android mobile device is a Google Pixel 3A running GrapheneOS. The steps to configure my device were very similar to the previous pages. Since GrapheneOS only supports Pixel devices, I decided to devote the previous pages to LineageOS, which supports hundreds of phones, in order to appeal to a wider audience. Please do your own research and choose the best platform for your needs. Either option is much better than any stock Android OS. Neither LineageOS or GrapheneOS connect to Google servers during a default installation.

RSS Feeds

I rely on Really Simple Syndication (RSS) feeds for the majority of my internet research. RSS allows us to fetch data from our favorite blogs and services without opening a browser; navigating through pages; allowing numerous tracking scripts to jeopardize our privacy; and being bombarded with ads. While I prefer **Vienna** (vienna-rss.com) for Mac and **FeedReeder** (jangernert.github.io/FeedReader) for Linux, I will provide the demonstration here using **Thunderbird** (thunderbird.net) due to compatibility across all operating systems. I encourage you to find a client which works best for you. All three of these are free and open-source.

First, assume you have found the blog at krebsonsecurity.com. You could bookmark this page and return on occasion to see if the author has added a new blog post. Instead, I recommend adding the RSS feed URL of krebsonsecurity.com/feed to your RSS reader. It will then notify you when a new blog post has been added. In Thunderbird, conduct the following.

- On the welcome screen, click the "Feeds" option and provide a name for your feeds.
- Right-click the new folder in the left menu and select "Subscribe".
- Paste the blog URL into the "Feed URL" field.
- Enable the "Show the article summary instead of loading the web page" option.
- Click "Add", enter any additional links of interest, and click "Close".

Thunderbird now displays the most recent blog posts from this site and will fetch any new posts as they become available. If you were to visit the site at krebsonsecurity.com every day, it would load Google Analytics by default which would track your internet activity. It would also download ads to your browser cache. If you view the RSS feed content without fetching each entire page, any JavaScript from the target site is not executed. You also receive the content of various posts without any advertisements, auto-play videos, and other nuisances. This is only the beginning of the capabilities of RSS feeds.

The previous example provided a direct link to the RSS feed (krebsonsecurity.com/feed) at the top of the home page. Other sites may not have an obvious URL present and you will need to identify the most appropriate address. Some clients, such as Vienna, attempt to identify the correct RSS URL when you submit a website home page. Others, such as Thunderbird, require a precise feed address. Because of this, and the outdated appearance, I typically do not recommend Thunderbird for RSS use. When I submit my own blog address of https://inteltechniques.com/blog/ to Vienna, it knows to translate it to a specific RSS address of https://inteltechniques.com/blog/feed/. When I submit the blog address to Thunderbird, it presents an error and does not try to translate to an RSS feed.

This brings us to the necessity to locate RSS feeds when they are not provided within the website. The following should assist.

- Most WordPress sites store the RSS feed in a subfolder titled "feed" at the root of the blog. If you had found the ProtonMail blog at https://protonmail.com/blog, you would only need to add "/feed/" to the end of the URL in order to possess the full RSS link (https://protonmail.com/blog/feed/).
- While on any website, press cmd-f (mac) or ctrl-f (Windows/Linux) and search for "rss". This may present a link to the RSS feed for the site. If this fails, right-click on the page, select "View Source", and conduct a search through the source code.
- Most news websites provide an RSS feed of their articles, but few advertise this on their home page. If I want to subscribe to feeds at the Los Angeles Times newspaper, I must conduct an online search of "LA Times RSS", which displays their RSS page as the first result (https://www.latimes.com/feeds). This page contains all RSS feeds available. Replicate this for any online news source of interest to you.
- Many podcasts do not provide a direct RSS feed and insist on subscription through Apple or Spotify. I prefer to load these feeds through my RSS reader in order to avoid listener tracking. When I cannot locate a pure RSS feed, I navigate to **Get RSS Feed** (getrssfeed.com). Copy any podcast link from podcasts.apple.com and paste it into this service. It presents the podcast RSS feed ready for import into your client.
- Identify third-party RSS services which assist with creation of feed URLs for the topics of interest to you. **Queryfeed** (queryfeed.net) can assist with Twitter RSS feeds of profiles and search terms while **Show RSS** (showrss.info) generates feeds which notify you when your favorite television shows have been released. There are many free services waiting to assist you.

In my RSS client, I have hundreds of feeds from blogs, Twitter, Reddit, and news websites. I spend more time in my RSS reader than my browser. I quickly digest my interests every morning similar to a newspaper. It may take some time and research in order to identify the RSS feed URLs from your favorite sites, but this only needs to be completed once. My favorite way to use RSS is with Reddit. I don't like going to the Reddit website due to the overall negative and toxic environment, plus dozens of trackers being forced to my browser, but I want to stay updated on the content. The following RSS feeds should help explain my usage.

New posts from /r/Privacy: https://www.reddit.com/r/privacy/.rss
Top daily posts from /r/Technology: https://www.reddit.com/r/technology/top.rss?t=day
New posts containing "bazzell": https://www.reddit.com/search.rss?q=bazzell&sort=new

You can create your own feeds from these examples. My reader currently has 214 feeds. The posts arrive in a format similar to email messages. I find this presentation better for my sanity, as it stops me from clicking links all day throwing me into various internet rabbit holes. If you have an interest in this tactic, please listen to episode 172 of my podcast which explains more. Figure 16.02 displays the folders, feeds, and content within my Vienna client.

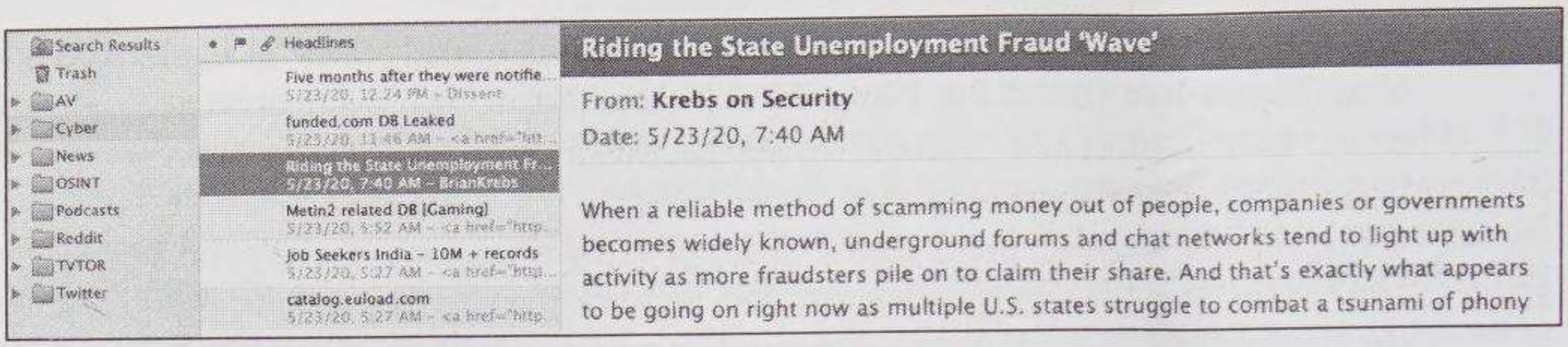

Search Results
Trash
AV
Cyber
News
OSINT
Podcasts
Reddit
TVTOR
Twitter
Headlines
Five months after they were notifie...
funded.com DB Leaked
Riding the State Unemployment Fr...
5/23/20, 7:40 AM - BrianKrebs
Metin2 related DB (Gaming)
Job Seekers India - 10M + records
catalog.euload.com
Riding the State Unemployment Fraud 'Wave'
From: Krebs on Security
Date: 5/23/20, 7:40 AM
When a reliable method of scamming money out of people, companies or governments becomes widely known, underground forums and chat networks tend to light up with activity as more fraudsters pile on to claim their share. And that's exactly what appears to be going on right now as multiple U.S. states struggle to combat a tsunami of phony

Figure 16.02: An RSS reader application with folders and feeds.

After you have your RSS client configured as desired, be sure to export your settings. Most clients have an option to export an Outline Processor Markup Language (OPML) file. This archive includes every RSS feed which you have added into your software. If you ever need to reconfigure your RSS client due to a hard drive crash, new operating system installation, or computer upgrade, this single file restores all of your hard work. I store mine within my VeraCrypt container, as previously explained.

Some readers may question the need for software clients when online RSS services, such as Feedly, simplify the entire process. While it is much easier to allow an online service to configure your subscriptions and host your settings, you sacrifice privacy. As an example, Feedly openly admits it collects your name, email, and any billing information upon registration. From there, it associates your interests, IP address, browser type, ISP, access times, crash data, browser cache, pixel tags, and various analytics to your profile. Use of their service allows them to share all of this data with third-party companies and social network sites. When using a trusted RSS client, your data is not shared with any online services, aside from the feeds to which you subscribe. A name, email address, and billing information is not needed with the clients mentioned here.

RSS feeds may not be considered "advanced" to most people, but I struggle to convince my clients to give them a try. While it may seem awkward at first, digesting your online content in this way can be very beneficial. It allows me to quickly identify posts of interest while skipping items I wish to avoid. Please note that all sites will still obtain your IP address, so be sure to always use a VPN.

I realize that most readers of this book will not apply all of the strategies presented here. It can be quite overwhelming to tackle all of this at once. I hope you return to this chapter as you progress through your privacy journey. Whenever you have a thirst to add something new to your arsenal, these topics may scratch that itch.

Chapter Seventeen

My Successes and Failures: Jane Doe

I wish I could tell you this life has been easy. I wish I had a guide for all of this while I was experimenting. I have been forced to test new strategies on myself, and occasionally clients. I have made my share of mistakes, and I have learned valuable lessons from each. These next few chapters serve as final tales of my various successes and failures when trying to make people disappear. I hope that these true stories provide insight which will aid the creation of your own privacy strategies, and give you a final confidence boost to achieve any level of privacy you desire. Obviously, all of the people mentioned have given consent to share these stories. I have redacted and modified many details to protect their identities. First, we meet Jane Doe.

I received an email through my website from a man that only asked if he could speak to me over the telephone about a sensitive situation. The name he used was the same as a fairly wealthy individual who served as an initial investor in a few successful businesses. His area code matched the general location of the investor, and his email address had a domain associated with a company that was registered to him. I scheduled a call for the next day. Those who have read my other books will know that I take every layer of my privacy very seriously. I would never call anyone from my actual cellular telephone number, and I try to avoid using Google Voice for anything too sensitive. Google keeps a log of all incoming and outgoing calls forever, regardless if the history was deleted by both parties. I also never call a cellular number of a potential client. I have no way of knowing whether the person's phone possesses malware that records calls and text messages, forwarding them to the adversary. The metadata of all calls and messages is stored by the service provider and a subpoena could make record of our communication admissible in a civil court. Instead, I instructed him to use the application Wire, which was discussed previously in this book.

I asked him to install Wire to a computer which he was confident had not been compromised, and not a mobile device. He would need to create an account and email me the username chosen. I would then call him through this app at a specified time for an audio call. While video calling is supported, I have no idea of what I am getting myself into. I don't want a stranger to save a screen capture of my face and later post it on the internet. I know that sounds a bit paranoid, but it is better to be safe than sorry.

We connected on Wire and made brief introductions. He was a savvy business person that knew how to get directly to the point. He stated that his daughter was in a true mess and he had no idea what to do. She had recently terminated a long-term relationship with an abusive man. The former companion was extremely upset and unstable. He confronted her at a friend's home where she had been staying and attempted to abduct her. She fought and was injured slightly during the process. She has always turned to alcohol and drugs to fight stress and was in a rut dealing with a boyfriend turned stalker. No matter where she stayed, he knew where she was. When she went out, he was there soon after. He even approached her in a grocery store demanding that she take him back before he "really" hurts her. She felt her world was out of control.

I asked the potential new client what level of help he was seeking. He immediately responded "the full treatment" and asked how quickly I could help. He wanted me to relocate her to a safe place where the boyfriend could never find her. He did not care about the cost, and assured me he would pay any expenses. We set up the details of establishing a retainer that would allow me to start getting things in place. While he was funding this adventure, I did not consider him to be the client. I advised that I needed to speak with her directly to start a plan and identify how exposed she was. He agreed to allow her to use his Wire account from his device and we arranged a call for the next day. Before we terminated the secure communication, I asked for the name of the boyfriend and as much detail about his life that could be provided. He only knew a name and occupation, which was plenty to start my own stalking.

"Chris" was a 30-something computer systems administrator who appeared tech-savvy. His Facebook and Instagram pages were decorated with photos of network cabling installations. This is often referred to as "cable porn", and hi-tech people are fascinated by routers and switches which possess perfectly installed network cabling, often hundreds of strands of wires. He had a GitHub page which tells me he understands technology more than the average stalker. This was most concerning as it often means that malicious software was installed on the victim's devices.

I was glad that we would be communicating on her father's computer. Chris had a cellular telephone number associated with his Facebook account, and a password recovery attempt identified the last two digits of the number. A search of his Instagram username on the website FindMySnap.com, which is now retired, revealed that a SnapChat username existed identical to the Instagram account. Furthermore, this SnapChat name had been in existence since prior to 2013 when a data breach leaked user information to the internet. This revealed the first eight digits of his cellular number. Combining the SnapChat and Facebook results revealed a potential entire cell number. Placing this number with country code into the Facebook Messenger app confirmed that the number was connected to his profile. This confirmation allowed me to further investigate his online presence.

I created a virtual Android phone using software called Genymotion which allowed me to use mobile apps on my computer. I placed his cellular number in my contacts phonebook within Android and left the name as Chris. I then installed several popular social networking applications on the device and executed the "Find My Friends" feature on each. This revealed the networks where he has profiles as most require a cellular number to establish the new account. I now had a good understanding of his online activity which would later prove to be valuable.

During my call with Jane, she seemed extremely scared. She said that he will never give up and that I was probably wasting my time. She knew he would find her and continue to harass her no matter where she went. She had given up on me before I could explain my process. I asked her what type of phone she had and where she got it. She stated that she had a Samsung Galaxy S6 and it was given to her by her former boyfriend. She confirmed that there were no Samsung stock apps anywhere, which convinced me that he had "rooted" the device. I had a strong suspicion that he had installed malicious software (malware) on her phone which was allowing him to see her location at all times. He could likely monitor her communications which would identify the friends with whom she had been staying. I advised her to keep the phone on, and send it to me via overnight Fed-Ex at the hotel where I was staying. I told her to go to an Apple Store, with her dad, and pay cash for a new iPhone of her choice. After purchase, I instructed her not to open it and call me on Wire from her dad's computer when ready to turn it on for the first time. She agreed.

While waiting to analyze Jane's phone and talk with her on a secure line, I decided to also dig into her life a bit. Similar to how I investigate the offenders of the situations with which I assist, I also conduct a thorough review of the victims. Early in my new privacy career, I was approached by a woman in her twenties requesting help hiding from her abuser. "Martha" explained how he was mentally and physically abusive to her and their young child. She did not feel safe and knew he would try to track them down wherever they went. I was eager to protect her from a future attack.

I began planning her move and made sure that there would be no trail that he could follow. I assumed that only women could be victims in these types of scenarios. It never occurred to me that she might be the problem in the relationship. Fortunately (and accidentally), I found an old Facebook post made by the father of the child. It displayed a screen capture of a court order allowing him full custody of the child. I could not see the details of the order, but the father was very excited that this day had come. I finally located the full court order which detailed the mother's drug abuse, child neglect, and three documented occasions where Martha tried to abduct the child and leave the country. This led me to court documentation about her mental issues and previous confinement for parental abduction. I confirmed that the father had full custody of the child, and that a police report was made three days earlier

about the mother failing to return him. I immediately contacted the father and local police in that area. I learned a valuable lesson, which is to always research both the victim and offender.

While researching Jane, nothing appeared out of the ordinary. She loved social media, and possessed very active Facebook, Twitter, Instagram, and Etsy pages. It was easy to see how she could be tracked based on postings from every location which she visits. If unable to find her based on live posts, her online history quickly developed a pattern of behavior that could be used to assume her current location. She appeared very close with her family, and a bit spoiled by her father. As a family with means, she obviously never went without any luxuries, and large gifts for every occasion were normal in her life. My immediate concern was that she would not be able to give up the online activity in order to protect herself. She was accustomed to immediate selfies the moment she receives a new gift or lands at a new vacation destination. She was in for a rude awakening.

That evening, Jane called me from her father's Wire account as instructed. This time, we connected via the video chat option. I wanted to assess her demeanor and look for visual signs of physical abuse. She was very shaken and had slurred speech. Her father warned me before the call that she had been drinking alcohol heavily lately, and today was no exception. He firmly believed that she would sober up once she was safe. As we talked, her father stayed right by her side, which was a problem. She was holding back details that she did not want him to hear. I politely requested to talk with her alone, which he prohibited. He quickly reminded me that he was paying for my time, and that he would be involved in every step.

I instructed her on how to turn on her new iPhone without attaching it to any previous accounts. I had already created her an anonymous Apple account that would allow her to download any basic apps and updates that she might need. We configured the Wire and Signal apps on her new device, which she could use over Wi-Fi only at this point. I had already ordered her a new Mint Mobile SIM starter pack from Amazon that would arrive at her father's house the next day. She was instructed to send me the details of the card, and I would activate it online for her. She would only need to enter the SIM card into her phone and have a clean device ready for communication. We would finish setting up the phone the following day.

Her father insisted that she would be safe at his home for the rest of the week. While the boyfriend likely knew she was there, he had never made contact at that location since the break-up due to the father. He was not shy to pick up a weapon at first glance of Chris entering the property. I knew that the father would likely be at work the next day, so I ended the conversation until then. I hoped that I would be able to talk to Jane alone in order to get the real scoop.

The next day, I received a Wire message from Jane stating that she had the SIM card and was ready to activate. We connected over Wire and finished the process. She was alone in the

house, which gave us an opportunity to talk candidly. Over the next hour, I learned details about her life which her family would never want to know. I learned about the hard drugs, the weekly routine of passing out and waking in an unknown bed, and the monthly breakups with Chris. She told me of the two occasions in which he raped her, which she never reported. She showed me the scars from the cigarette burns purposely placed on areas of her body normally covered in clothing. I asked the difficult questions such as why she continues to go back to him. She answered honestly with "for the drugs". Chris was not only her lover, but also her drug dealer. She was allowed a non-stop buffet of various drugs in return for their relationship. Chris needed to go away for many reasons.

Jane was adamant that she was ready to go to rehab and leave Chris permanently. He had told her on numerous occasions that he would kill her if she ever left him and that he would never stop hunting until she was dead. He was mentally unstable, fueled with drugs, and possessed a large amount of cash from his illegal transactions. He was a valid threat. With her father funding the privacy campaign, I was ready to execute various strategies. The first priority was to get her the help she needs. It was time for rehab.

Sending Jane to rehab sounds like a simple task. Drive her there, drop her off, and send the bills to her father. It was not that easy. In Jane's part of the country, there were not many rehab options. Chris would have no trouble contacting each facility and using social engineering tactics to identify the location of her stay. For those that are not familiar with the term, social engineering is psychological manipulation of people for the purpose of performing actions or divulging confidential information. It can be simplified as lying during a con. I have used this tactic many times on behalf of clients.

A call by Chris to each rehab facility during a weekend evening, when newer staff is likely to be present and administrative personnel are not around, consisting of a few targeted inquiries, is likely to quickly identify her location. "Hi, I am Jane's brother. I was there earlier today to visit, and I left my inhaler there, do you have it? I can't get a replacement until Monday". This will be met with either, "We don't have a patient here with that name", or, "I don't see anything at the desk, let me go check her locker". Chris would be in her room within hours. She would be either dead, kidnapped, or sedated with illegal drugs before sunrise.

I convinced the father to place her in an out-of-town rehab facility that often caters to celebrities. These institutions are more likely to block amateur attempts at obtaining patient information. They know the tricks and are suspicious of every phone call. Their security is better than the average clinic and the place I chose does not allow any cellular devices within the buildings. He agreed, and she began packing. This was equally beneficial to me as it would give me time to set up her new life.

I purchased Jane a one-way airline ticket to the city of her rehab using a prepaid credit card purchased from a local CVS pharmacy. I chose the Vanilla Visa reloadable option. The maximum card value available is $500, but an additional $2,000 can be added to the card each day in $500 increments. Therefore, I can walk out of the store with a $2,500 balance on the card. Why not just use her real credit card? I must assume that Chris has access to her statements and activity. A simple keystroke logger on her laptop, or malware on her previous phone would give him her passwords. Monitoring her credit card activity would tell him the flight number, which would identify her future location. This would give him a great advantage. Today, airlines are more cautious with prepaid card purchases. If replicating this today, I would use a Privacy.com account.

I hired a car service to transport her from the family home to the airport. Before picking up Jane, the car would pick up Jane's escort, an off-duty police officer from a neighboring community. For several years, I had been teaching open source intelligence (OSINT) techniques to local, state, and federal law enforcement agencies all over the world. This has created a massive private list of contacts covering most areas of the country. I reached out to a woman who I had met at a class and asked if she would be willing to take a day off of work in order to make some side income. She agreed, and escorted Jane to the TSA checkpoint.

The reason for the escort was two-fold. First, I wanted someone with Jane in case Chris appeared during transit. I also wanted that person to be armed with a gun and have the training to use it. While this scenario of Chris intercepting transport is extremely unlikely, I prefer to be prepared. The more likely reason that this officer would be needed is to make sure that Jane makes it to her flight. I still did not trust that Jane would not willingly disappear looking for drugs. I would expect to hear that Jane never made the flight. Therefore, her escort was there for the entire process, and even waited at the only terminal exit until the flight had taken off. I was happy to give this officer twice her daily wage for a few hours of work.

Upon landing, I repeated the process with an off-duty officer working for the airport police department of that area. He picked her up at her flight's gate and escorted her to the vehicle service, then the vehicle, the entire ride, and to the front door of the rehab facility. I received text updates throughout the entire day. Everything went as planned, there were no hiccups, and Jane was safely at rehab. The security team there was now in charge of her. This is one of many reasons that I try to collect as many business cards as possible at my live training events. Contracting local off-duty police officers is my preferred option every time, especially those that I have met during my classes.

Now that she is safe at rehab, my work begins. I must secure permanent housing for her, as she may only be in rehab a few weeks. This is where I try to provide value to my clients. I establish a new life that they can simply walk into without much effort. I create new aliases and establish believable histories that allow people to feel safe in their own homes. It is vital

that any actions I take associated with Jane's new life have no attachment to her previous existence. This is easier said than done.

The first step is to establish housing. Jane's situation is an ideal case for renting. Her father will pay the rent, and she will not stay at this new place long-term. When I create a relocation plan that includes a rental property, I always plan for the client to be present at the location for one year. In most situations, they relocate to something more permanent before the year is up. On rare occasions, they need to extend their situation past the first year. Compared to the purchase of a new anonymous property, establishing a rental unit is much simpler.

Since I will not be providing my client's name or personal details, the thought of obtaining a commercial apartment is out of the question. These large complexes are always controlled by a third party or national chain. They will always require a full background check including the client's SSN and DOB. An occupancy permit will be filed with the city or county, and there is no way to establish privacy in these situations. Therefore, I always focus on properties available for rent by the owner. Preferably, I desire small homes situated on the owner's primary residence property. Since the owners will always be physically next to the unit being rented, they know that they can keep an eye on things, and have a stronger sense of control over the property. This tends to give them a sense of security and in return lowers their concerns to overly vet a new tenant. In a small town, finding these properties requires an afternoon drive and a keen eye for signage. Larger cities require the internet.

Zillow does not offer a specific search for rental housing available strictly by owner. However, a few tweaks can eliminate the larger commercial properties in which I have no interest. After selecting "Rent" from the main page, I select "In-Unit Laundry" from the "More" tab. This eliminates many of the multi-unit properties that share a common laundry area. I then deselect everything but "Houses" on the "Home Type" option. This works best on most areas, but will not work on extremely populated urban areas. I always guide my clients toward areas with a bit of privacy, such as a standalone residence. I then compare the areas of interest to various online crime maps in order to identify the safest area of town. Identifying homes that would be acceptable to the client is not the hard part. Finding landlords that will play nicely with my antics is the difficult piece.

Once I find a home of interest, I contact the owner in person. I arrive well-dressed and in a newer rental vehicle. I politely tell them that I am searching for a friend, and that we are ready to rent right away. I am usually met with an application at this point, which is when things will go one of two ways. My first few attempts at obtaining anonymous housing for victims were disasters. I incorrectly assumed that the landlords would be fighting over me and the money. I strongly stated that I would not disclose the name of the tenant and that we would be providing no identification. You can guess how that went. I slowly learned that a specific delicate approach tends to work most often.

In this scenario, while home-searching for Jane, I found a perfect one-bedroom house tucked back in a wooded area. The home sat on the corner of three acres, opposite of the property owner's home. The home was vacant, and the owners proudly walked me through the recent updates. It was then time to lay out the situation.

I advised the couple, both retired and in their 60's, of the situation. I disclosed my real name, and offered them my retired credentials and badge to verify my identity. I also advised they could Google me and confirm the type of work I conduct. I informed them that I am seeking a small quiet home for a woman that has suffered a lot of mental and physical abuse. She has become fairly skeptical of the world, and has asked me to deal with housing. It is vital that her name is not associated with the home or this address, and it is a matter of her own safety. It could literally be life or death.

As I saw the brows of the owners display the concern on their minds, it was time to sweeten the deal with the following statements. "I realize that you will be very strict when selecting the tenant for this amazing property. I truly hope that you will consider her, as she would be a respectful and quiet tenant. I know the situation is unique, and I would share your same concern if I were in your shoes. This is why we feel the need to compensate you for your consideration. I am authorized to pay the rent in cash each month, plus a deposit, and prepay three months of rent as a gesture of appreciation". This usually converts the look of concern to images of cash in their pockets. While this does not work every time, it usually opens the door for further negotiation. On one occasion, a landlord responded with "Make it six month's cash, in advance!" I happily agreed and my attorney handled all of the paperwork.

This brings up an important point to consider. Obviously, the client's name does not get associated to the property whatsoever, but neither does mine. I have property attorneys on each coast that take care of all rental paperwork and happily attach their own names and signatures to any forms. Neither of them cares about their own privacy, they each use their public office addresses, and neither of them ever know the identity of my client. They each receive a nominal fee for their one or two hours of light paperwork (which they likely have an intern complete).

At this point, you may be thinking that this all only happens because the client has money to throw at the problem. While this is true in this situation, it is not always the case. I have had many clients that did not have a penny to pay, but still received my services without charge. I have also had extremely wealthy clients that pay the lion's share of the bills.

The owners agreed and I now had a rental property lined up for Jane. Two days later, I had the keys and legal possession. During the previous walkthrough of the property, the power, water, and gas was active. I knew that utilities were not included, but I incorrectly assumed that the bills would stay in the name of the property owners. This had been the case with my

previous client relocation, and the landlord just added the usage to the monthly rent. This is always the optimal route to go. In hindsight, I was so excited that they agreed to waive the background check and application process, that I got ahead of myself and just wanted to get a contract signed. This was not a huge issue, but I was very disappointed that I had not clarified this. As I stood in the living room of Jane's new home, I was without power or water. All utilities had been terminated as of the move-in date.

The next morning, I first contacted the power company. This is never an easy call. Traditionally, establishing power to a residence requires a "soft pull" on a person's credit report, which demands a Social Security Number (SSN) of my client. Some may wonder why I would not want to share this information with them. The simple answer is that the details provided will absolutely become public record at some point. Data mining companies often obtain utility records in order to better populate their databases on practically every citizen. The name on the utility bill will likely be present on free people search websites within ninety days. Therefore, disclosing my client's identity to the power company is not an option. Instead, I will test the waters one piece at a time.

Since I record all of my telephone calls as they relate to a client, I am able to provide an exact transcript of the conversation. The following occurred in Spring of 2017.

Operator: Hello, how may I help you today?

Me: Hello, I need to activate power at my residence, can you assist?

Operator: Absolutely. What is the address?

Me: REDACTED

Operator: OK, I do see that this address is part of our coverage area, and that power was terminated on Tuesday. When do you want the power activated?

Me: Right away if possible, we are moving in today, and my daughter is so eager to get the PlayStation going.

Operator: What is your name sir?

Me: John Arthur Wilson

Operator: And what is your date of birth?

Me: Hmmm. I really hate to give that out, I was the victim of identity theft this year, and the officer advised to never give out my DOB or SSN. What are my options?

Operator: Sir, I cannot turn on the power without your information including your social.

Me: Oh boy, that is concerning. I am happy to pay a deposit to my credit card in order to bypass this valid requirement. Is there a supervisor that can authorize this?

Operator: Sir, I can tell you most certainly that we cannot turn on the power without your full information. A supervisor will tell you no different.

Me: Understood, let me call you back after my wife gets home.

This conversation was typical. Utility companies want to be sure that you do not rip them off and leave with an unpaid bill. By conducting a credit check, they can come after you when you owe money. In about half of my attempts, I am allowed to pay a $250-$500 deposit in order to bypass the credit check and SSN requirement. Usually, I can provide a credit card to pay this, but sometimes they will want a check mailed. I am prepared for either scenario with a secondary credit card that I maintain in an alias business name or a check with no personal name or details in the upper left corner. Both are valid payment, and connect to a business checking account in the name of an LLC that I maintain solely for this purpose. I then invoice the client for these expenses.

After waiting a few minutes, I called the power company again and was given a different operator. The conversation was similar, but I took it a new direction, as follows.

Me: Yes, I am trying to help a foreign exchange student obtain power at a rental home. My English is a bit better than hers, so I thought I would assist.

Operator: What is her name?

Me: REDACTED TRADITIONAL INDIAN NAME

Operator: Does she have an SSN?

Me: No, she says she has a UIDAI National Identification Number, can she give you that?

Operator: Sure, go ahead.

Me: 5485 5000 8000

Operator: OK, so, just so you know, she is going to have to pay a $200 deposit, which can be refunded after one year or when she terminates service, does she have a credit card for this?

Me: I am happy to pay that for her, are you ready for the number?

Everything was smooth after that point. Before you judge me too heavily as a fraudster, let me explain. The Indian government assigns a twelve-digit national identification number called a Unique Identification Authority of India (UIDAI) number. On their website, and an example of this number is displayed on a fictional card as 5485 5000 8000. This number will never be assigned to any individual. Furthermore, the U.S. utility companies have no way of verifying this number as valid. Operators likely just add it in the notes section to cover themselves.

Think about it. Thousands of foreign exchange students enter colleges and universities every year. They all live in some type of housing that requires utilities. Most of these require the student to pay the utilities directly. Therefore, it is a common occurrence for non-U.S. citizens to activate power at a residence. Starting with this excuse has been more successful than trying to make an employee understand that you prefer not to identify the homeowner. At the end of the day, all of the bills are paid, we have stolen nothing, and the utility companies are happy. No one ever checks up on this situation because there is no need. I make sure the bills are always paid in a timely manner.

The water, sewer, and trash services were much easier. After they were notified that the power had already been activated, they seemed content that everything was legitimate. I set all three services to auto-pay to an anonymous debit card created specifically for this client, and provided a very generic name. I used Privacy.com, as explained previously, which connects directly to the victim's personal checking account. After association, users can create an unlimited amount of debit card numbers, each used for a single merchant. Any billing name and address can be used during payment, and the transactions are withdrawn directly from the checking account on file. The merchant (utility company) does not know the true name of my client. The service (Privacy.com) does know the name of my client, but does not know where she lives. They only know that she pays various utility companies monthly. There is obviously a paper trail here that could be identified with a search warrant or court order, but those are not my concern. I need her out of public view.

The house was ready for Jane in plenty of time for her release from rehab. It was now time to train her on the use of her new aliases. Choosing an alias name can be difficult if too much effort is wasted on finding the perfect option. I don't buy into that, and I don't get overly creative with picking aliases. Why does she need an alias name? She can never associate her true name with her residence. She will need something to use in place of her given name.

I almost always recommend that a client maintain their actual first name as part of their alias. The exceptions are very unique names which would be easy to find with targeted searching. Jane is a common name, so it will work fine. Also, she will naturally respond when called, and will not create an awkward situation when she can't remember her alias name. She cannot ever use her last name, so I often recycle the last name of either the previous resident or the landlord. In this case, assume that the previous resident was also named Jane Doe. This would not work, as it is too similar and mail could be accidentally forwarded to the previous resident. If the previous resident was named Jim Watkins, Jane Watkins could be a good choice, unless Jim has a family member with the same name. A quick search through various people search tools immediately identifies relatives' names. If the previous resident's last name is not working out, or is very unique, I will focus on the landlord's last name. In this case, the landlord was Matthew Parker. Therefore, Jane Parker will work great.

Why not choose a random last name? There are a few reasons, but the most important is familiarity. If Matthew Parker owns the property, and is publicly listed on many websites, another person there with that last name is not suspicious. The mail person will not think twice about delivering mail to a person with a last name matching the property owner, who also receives mail on occasion. Also, it helps hide the fact that a new resident is present. If this is a small town, it would not be difficult to search for any new residents within the past month. This could unnecessarily expose my client. Maintaining the last name of the property owner or previous resident is just much simpler. There is one other reason.

In a perfect world, my client would only pay with cash, buy all necessities from the local store, and never attach her real name with any purchase ever again. We don't live in that world. We require Amazon accounts with Prime shipping, and practically every big-box store will require a name and other details for large purchases and deliveries. It is almost always certain that the databases that store these details will be breached, sold, or somehow released publicly at some point. Therefore, we must be prepared.

First, I created a new Amazon account in the name of Jane Parker. I supplied the real address to her home, and Amazon conducted a public records search as part of its fraud prevention actions. Having the last name of the property owner can often bypass any red flags present when it can't verify Jane Parker is a real person. Amazon seemed happy with the details, and the account was ready for funding. I did not provide a Privacy.com masked debit card number to this account, as these are detected by Amazon as suspicious when attached to a new account. Instead, I purchased an Amazon gift card from the closest grocery store to the residence. Amazon knows where these accounts are purchased, and buying in one state while using in another is also a red flag.

I attached the Amazon gift card to the account and made a small purchase. This is below the threat model that scrutinizes first purchases, and I selected the option for a free month of

Amazon Prime. The item arrived quickly, and my client now has history with her new alias and new address within their system. I chose the option to purchase Amazon Prime for an entire year and used the remaining balance of the Amazon gift card to pay the fee. This makes Amazon happy, and their systems become much less cautious of the account. At this point, I add a new Privacy.com masked card to the account and make it the primary form of payment. Jane can use this account to buy anything she wants from Amazon, and the transactions will be withdrawn from her personal checking account behind the scenes.

This process can be replicated with any other online shopping options, choosing a new Privacy.com card for each purchase. Within a few months, data mining companies will assume Jane Parker is real. She will even start receiving junk mail at the house. I see this as a sign of success. She has committed no crimes, compromised no one's identity, and paid all of her debts. She has no photo identification including this name (yet) and will never identify herself as an alias to any government official. She knows the rules. More importantly, she will never tell anyone she does not know that she is Jane Doe.

Using an alias on the internet is easy. Online shopping is an interaction between your computer and another computer. Neither cares about much except whether you have a valid form of payment or you are a fraudster trying to rip someone off. As long as we keep the systems happy, we will likely never be stopped. In-person purchases are a bit trickier. In my youth, I paid a cash deposit for my first apartment, and wrote a check at the local furniture store for a couch and kitchen table. I was never asked for identification. Today, paying cash for large items is criticized and any large purchase requires a valid government ID. Let's tackle both of those issues.

Now that Jane was healthier, I snapped a few boring face-forward photos of her standing in front of a white wall. Each had her wearing a different shirt and her hair in a unique style. These will be my starting point for creating her first ID in her alias name. Before you get bothered by this, please let me explain. There will be very rare instances that she will need this, and we will be sure not to break any laws during the creation or utilization of these IDs.

When we think of "Fake IDs", we often have thoughts of underage kids buying a poorly made driver's license with an unbelievable date of birth. That illegal act is never tolerated by me in reference to alias IDs for my clients. Instead, I strictly use the following guidelines which are repeated from an earlier chapter. Please note that some state laws vary, and that I am not an attorney.

LEGAL: Non-government identification in an alias name can be legal. There should be absolutely no mention of any state or the word government. There should be no mention or reference to any real businesses. It should not identify you as an employee of a legitimate company.

NON-LEGAL: Any false identification that displays the words city, county, state, government, police, license, driver, court, agent, et cetera is a crime. This should be obvious. Any reference to employment by any government agency is also illegal. If any part of you thinks that you might be crossing the line, you probably are. Please stop.

I hesitate to discuss the option of printing my own alias identification cards in detail because people may try to break the law and create fake government IDs. Lamination machines and holograms are very affordable on Amazon and local print shops will happily laminate anything you print yourself at home. There are many templates of various styles of photo IDs online, but most are illegal. For Jane, I have a legal solution in place that will assist with convincing others of her new alias name. I made her my employee.

I own a legal LLC business entity that accepts no income whatsoever. Therefore, it does not require an EIN with the IRS and there are no tax reporting requirements. It has a very generic name that could apply to many different industries, similar to Premier Solutions LLC. Jane became a volunteer assistant for this LLC and received no compensation. As an associate of Premier Solutions, I demand that she possess an employee identification card with her photo and name. Since we are a very fun company, every employee chooses a "stage name", and Jane's happens to be Jane Parker. I created a new identification card through a template on my laptop, inserted one of the photos I captured, and printed the file to my IDVille card printer purchased from Staples. The ID was printed onto plastic card stock which had the same quality as many government issued IDs.

Possession of this card is not illegal but attempting to falsely identify herself as her alias to a government employee is a crime. Where would she need this? Checking into hotels and receiving packages first come to mind. I advised her to keep it hidden in a wallet, and never remove it unless absolutely necessary.

Aliases possess an unfair reputation as being shady or criminal. While this unfortunate use occurs, an alias itself is not illegal. As long as you do not cross the line of any sort of government identification, you can be anyone you want. It is not a crime to give another civilian a fake name. If I were to visit a Starbucks, I would not give out my real name. There is no benefit. If I entertain a group of clients at a restaurant, I do not provide my real name to the establishment. They do not need that. They only need payment for the services in the form of cash or a secondary credit card. I do not want my clients' true identities within their databases and guest books that will eventually be breached and leaked online. While this may seem overly cautious, I am aware of the daily breaches and intrusions into sensitive data stored by third parties.

When a client has a legitimate need for identification in an alias name, I encourage them to seek out their own IDs that can help "pad" a wallet. I have found many national chains of

gyms that issue a photo identification card that can be shown for entry into any gym location nationwide. I have had great success using this as a valid proof of identity at hotels. Many of these businesses will give you a 30-day free trial in order to evaluate the property. Of those that I have tried, some of them issued the identification card with photo. I have also found a handful of spas in affluent areas that possess a monthly usage business structure. These also mandate that members show their spa ID upon arrival, most with photo on the card.

Animal shelters are becoming more aggressive about security and often ask volunteers to wear an identification card while on premises. Obtaining an alias photo ID from a shelter as a volunteer has many benefits. First, volunteering and caring for the animals is a nice thing to do. Also, showing this ID when checking into a hotel often sparks a conversation with the receptionist about his or her animal history, and it creates a calm and welcoming environment sure to pacify corporate policies about valid photo identification.

Now that Jane had her invisible home, new alias name, and photo identification, it was time to issue her a new credit card. This is actually one of the easiest steps, which surprises many people. We wrongfully associate our credit cards with a belief that they can never be legally used by other people. Any of us can give a credit card to someone else and authorize them to make a purchase. While a merchant may not accept use without identification, there is no fraud. Similarly, we can use a credit card in someone else's name. However, there are some very serious caveats to this, as explained previously.

Many married couples possess two credit cards that are connected to a single account. They may possess the exact same account numbers and expiration, but they display different names for each spouse. One of these cards is associated with the PRIMARY account holder, while the other is a SECONDARY issue card. This can also be true for children. Many parents add a secondary card to their account, place the child's name on the card, ship them off to college, and hope for the best. If you have ever ordered a secondary card for an account, you have likely noticed that there was never an inquiry for an SSN for the cardholder. This is because it is only a secondary card. There is no need for a credit check because the primary card holder is responsible for all charges. Theoretically, you could add a secondary card in practically any name to an account, and any purchases with that card would simply appear on the primary credit card statement. We can use this as a strategy for privacy.

There are only a few major credit card companies that offer secondary cards without much resistance. Of those, Chase and American Express are two of the easiest. Unfortunately for me, Jane does not have either of these cards. Instead she only has a US Bank credit card. The major banks, such as US Bank and Bank of America will not issue secondary cards to an account without a full vetting of the new cardholder, including SSN. Jane was willing to apply for a Chase card, but I had just established her credit freeze, which prevents any new inquiries. This important strategy was discussed previously. Therefore, I had to un-freeze her credit,

apply for the new card in her father's address, and then re-freeze her file. This is not a huge deal but added a few days to the process. Once she had a new Chase card delivered to her father's address, it was time to add a secondary account.

An important step to this process is to never use the original card in the real name. Any secondary cards will have the same account number, and we want to keep a bit of distance between the names used. I immediately destroyed her card to prevent temptation. After instruction and a rehearsal, I had her call Chase about her account.

Chase Operator: Hello, how may I help?

Jane: Hi, I just received my new credit card, thank you so much! My previous provider issued me a second card for my step-daughter in college, is that possible with this card? I just want her to have something for emergencies.

Chase Operator: Absolutely, what is her name?

Jane: Jane Parker. She has my first name and her father's last name.

Chase Operator: Before issuing this card, I must make you aware that all purchases with this card will be charged directly to you and you will be responsible for all activity. Do you still agree to having a secondary card issued to your account?

Jane: Yes.

Chase Operator: OK, the card will arrive at the address on file to your account, it will be addressed to you, and will arrive in a plain white envelope.

In three days, the card arrived at Jane's father's residence, and she now had a credit card in her new alias name. There is obviously a connection between these two names now, but only Chase knows this. Chase will eventually include this new alias as a possible associate of my victim, but that cannot be avoided. Having a credit freeze in place will prevent the majority of this leakage.

I do not advise all clients to obtain a secondary credit card. The wealthy clients have many more options such as invisible LLCs with business checking accounts. However, Jane does not have the resources for this. Also, she will definitely need a credit card for daily life, and I do not want her using anything in her real name in the new town where she lives. Therefore, the convenience of having an alias credit card outweighs the risks associated with connecting a secondary card to an alias name.

The final step in Jane's plan was to establish a post office box in her real name at a small post office a couple of towns away from her. She will need access to mail and her bills, and nothing should ever be delivered to the house in her name. I helped her complete the form and supplied only legitimate information. I used her previous address, where she still receives mail, and her real name. The post office does not know her true physical address. Jane was instructed to only use this address for anything that she needed to receive in her real name. It should never be used for her alias. That would connect the two names together further and could jeopardize her home address by associating her real name to any alias utility bills. She could use this PO Box as her address for tax filing and any other government related services. It cannot be placed on her driver's license, but that is not necessary for her at this time. She was still listed under her father's address. Other clients have had to obtain a new driver's license address, often referred to as a ghost address, which was explained previously.

Jane was now in good shape. I was finished. She was clean and sober, lived in a house with no ties to her real name, possessed an alias ID and credit card, and most importantly had a strong understanding of the reasons for all of this fuss. I wished her well, and incorrectly assumed we would never see each other again. She would later reach out to me when Chris showed up.

I take responsibility for this. When I gave her the secondary credit card, I told her to use it sparingly, and only when a credit card was required. I focused on things such as hotels. I did not make it clear that the card should not be used as part of her daily life. As time passed with no sign of Chris, she relied on this secondary card heavily. She used it every week at the local grocery store and for fuel from the local gas station. The credit card possessed a very detailed history pattern. Chris identified Jane's new ProtonMail email address from a common friend. He then sent Jane a phishing attack for which she became vulnerable. She provided her ProtonMail password, which Chris used to access the account. In the archives was her credit card statement. He now knew the general area where she resided. Since he is a psychopath, he traveled to the area and secured a local hotel. He parsed through all of the property tax records for the county and isolated those that matched the properties marked as rental units with the county occupancy division. He now had a list of rental homes with each owner's information. He contacted each owner via telephone and provided the following script.

"Hi, I am Jane's brother. I would like to make her rent payment for next month on her behalf. Do I have the right landlord? This is a gift and I would like to surprise her, so I hope you will keep this a secret for now."

He assumed she would keep using her first name, and he was correct. Most of these calls ended with confusion as the owner did not know "Jane". Eventually he reached an owner which confirmed he rented to Jane and even described her to make sure they were each talking about the same person. He now had a likely address. He conducted surveillance but did not ever catch her in transit. Her recycling bin was in the street, so he removed the contents and

returned to his hotel. In the bags of papers and plastics, he located empty envelopes addressed to Jane at her PO Box. He knew he had the right home. That night he committed a home invasion and was waiting for her when she returned home. A physical attack ensued, he fled, and was later arrested by the local police. These details were gathered by a detective during an interview with Chris. The detective stated he seemed proud of his work.

I learned a lot from this incident, as I had made many sloppy mistakes. First, I underestimated the suspect. I now assume that every adversary is technically skilled and diligent. Next, I should have stressed more to never use any credit card, even a secondary alias card, near your home. This payment history displays a very unique lifestyle pattern that provides a great starting point to physical location. I should have had her purchase high-dollar gift cards from stores far from her home, and then use those if she needed digital payment. Better, I should have enforced the use of cash at all times.

Next, I now consider the alias first name. I usually like to maintain the first name of my client as an alias for appropriate response in social settings. This may not be wise for clients with extreme circumstances. This is especially important for those with unique names. I must now always include the landlord when considering the weakest links in my plan. I should have also stressed the importance of shredding or burning anything with her name the moment it needs to be discarded. Personally, I burn anything with sensitive information, but only after it has run through my cross-cut shredder. This makes for great kindling if you have a fireplace or wood burning stove.

Jane and I learned a lot. She was one of my first abuse clients. I was working in uncharted territory. This is no excuse; these were amateur mistakes with advanced adversaries. Jane has since moved to another home anonymously using similar methods as stated previously. She had one close call when her home address was published to an online marketing website which gathered "leads" through malicious methods. Her name and home address were leaked to this database because she requested a quote from a questionable online renter's insurance provider which shares data with numerous third parties. The data was later sold as leads for future business. This site had no opt-out policy and requests to the business owner went unanswered. My response was to file a COPPA complaint. I informed the website owner, copying the abuse address for his web host, that he was in violation of the Children's Online Privacy Protection Act (COPPA) by publishing the name and address of a child under the age of 13. I provided my adult client's details. The next day, the entry was removed. This was a bit shady, but warranted in my opinion. I have little sympathy for these types of sites, and I hurt no one. Surprisingly, this tactic works often when websites otherwise refuse to remove personal data.

Chris served less than a year in county jail for the home invasion, and he likely continues to hunt her. While I have much higher confidence in my new strategy for her, he still keeps me up at night.

Chapter Eighteen

My Successes and Failures: Jim Doe

When I became a police officer in 1997, I had absolutely no concern about personal privacy and safety. My home loan and property taxes were in my name, and all utilities were sent to me at the house. I was very publicly associated with my home and was even listed in the phone book. A few years later, I was involved in a high-profile case that made me question my transparency. While it took me a few years to get completely off radar, I was lucky that I never actually needed the protection. This is not the case for many police officers today.

I often get panicked emails or phone calls from cops that either attended my training or know someone else that had. Something has happened in their lives that has created a spotlight on them, and they realize too late that their entire lives are available online. This was the case of Jim Doe. Jim was a police officer in the U.S. that was involved in the shooting of a suspect during an investigation. The shooting was later found to be justified, but that did not matter much at the time of the incident. Before a thorough investigation could be conducted, the public and the media assumed that the officer was wrong and demanded immediate answers. Protests began and media coverage fueled the hate expanding through the city. The focus quickly turned to Jim.

Jim's department refused to identify the officer that was involved in the shooting until the investigation was complete, but that did not help him. Anonymous "hackers" began investigating the incident themselves. They identified all of the police officers from that city through public payroll records. They then eliminated those that were not on duty after personal social network posts displayed them in family settings. The officers on duty the night of the shooting were quickly identified. Calls to the station asking to speak with each of them resulted in the same officer never being available. Officer Jim Doe must be the shooter.

People began spreading Jim's name throughout social media, which the press picked up right away. Online searches through various people finder websites easily identified Jim's home address, phone number, and family members. News crews were stationed outside of Jim's home, hoping to capture a video clip of him walking to his car. Jim was stuck, and his family was afraid to leave the house. At night, protesters began throwing objects at the home and yelled threats toward the entire family. Jim's children could not attend school as they also received threats over the internet. Jim reached out to me for help.

This is a difficult situation. I can't make him and his family invisible overnight, and I can't make the world forget his home address. All I could offer was to help him obtain temporary anonymous lodging and some peace. At that point, we could create a strategy to get his life back in order. The first order of business was to get him and his family safely out of the house without anyone following. This could be difficult as the group of people standing guard at his house was growing every day. Simply driving him away from the home was not an option.

I contacted the local fire chief and explained the situation. He was very sympathetic, as the police and fire departments work together closely. He confirmed that the fire department possessed an ambulance crew as part of the service to the community. He agreed to assist with the safe relocation of Officer Doe. We identified a time during shift change when an extra crew would be available. This was to avoid any disruption of normal emergency service response. At that time, an ambulance with two medics responded to Jim's house. The lights and siren, which were only enabled upon arrival at the home, cleared a path through the aggressive crowd. The ambulance backed into the driveway until it reached the attached garage. At that point, an off-duty officer opened the garage door, which was almost touching the ambulance, leaving only a small opening that allowed visibility inside. Jim and his family loaded into the ambulance and it departed.

While the ambulance drove away, a police car followed slowly, creating a large gap between the ambulance and press attempting to follow. No one would pass the police car on the two-lane road, and the ambulance eventually disappeared. It responded to a pre-arranged meeting spot where a family member was waiting with a minivan. The family loaded into the van and then continued to a hotel the next city over. An unmarked detective car monitored the situation and confirmed that no one had followed the minivan. Step one was complete.

Jim's department photo was leaked onto the internet, and his face was plastered on practically every television in town. I did not want him recognized by anyone at the hotel. All it would take was one careless employee to tell the world where Jim was staying. Traditionally, this could present a problem, as Jim will need to check into the hotel and pay by credit card. Fortunately, there are alternative options for this.

Before Jim's arrival, I created a new Hilton Honors account online in a new alias name. I then made a reservation at the desired hotel using this account and alias. I used my own secondary credit card in order to hold the confirmation, but did not want to place the expenses on this card. Within moments, I received an email from Hilton with the option to check-in online and select a room. I completed this process through the Hilton website, which eliminates the need to present identification upon check-in. It is designed as a time-saving option, but rarely is. A physical credit card is still required upon check-in, which I did not have attached to Jim's new alias. Fortunately, this Hilton property offers electronic locks that can be opened through the

Hilton app on an Android device. Jim downloaded the app to his new burner Android phone, and logged in with the credentials I supplied to him. I needed to work on anonymous payment.

I could not simply use his real credit card as attached to his real name for the hotel payment. That was too risky. In order for him to rest safely, it was vital that no one could connect him to the hotel. Many of his co-workers offered their own cards, which was no better in my opinion. Instead, Jim sent me his credit card details, and I created an account with the online masking service Blur. Blur generates one-time use credit card numbers for any purpose. At the moment of creation, the chosen dollar amount is immediately charged to the real credit card. The benefit of this new masked credit card number is that any name and zip code can be used during any purchase. The disadvantage is the fees associated with each purchase. This would work fine in a pinch, but not long term.

I created a new virtual credit card in the amount of $500 and supplied this card to Jim's two-night stay. This action allowed me to prepay for Jim's room, which authorized his phone to unlock his room's door without ever stopping by the front desk. Jim and his family walked in the hotel, went straight to their room, and his Hilton app used his Android's NFC connection to unlock the door. The family was now staying in a hotel safely and anonymously. Very few trusted people knew their whereabouts. There was no media hounding them, protesters screaming at them, or rocks smashing their vehicle's windows. It was quiet and created an environment that could be used to regroup. I arrived the next day to begin planning his new privacy strategy.

Jim was obviously shaken, but not nearly as much as his wife. She was a wreck. Jim had the nerve for these types of situations, but it was killing him to see his wife scared. Earlier that day, she had received messages on her Facebook accounts that included manipulated images of her children inside coffins. Combine that with a family of four stuck in a typical Hampton Inn hotel room sharing one bathroom, and you have a stressful weekend on your hands. I don't know any parent that would not be upset.

There is no easy solution to this scenario. They can't stay at the hotel forever and will need to assume regular lives at some point. My immediate concern is always physical safety and short-term anonymous lodging, which I had achieved. The next step is mid-term housing which usually goes one of two directions. Either I establish an option that allows for a longer stay, or I identify friends or family that can support them while I figure out the next steps. Jim had no family homes where he would be comfortable staying, and his wife's parents had passed many years ago, leaving her as an only child. All of his friends were cops, which would never work. Placing them at a co-worker's home could either jeopardize the safety of that officer or further expose attacks to my client when angry protesters decide that any local cop is fair game. It was time to consider extended stay options.

In 2014, I was the keynote speaker at an insurance risk conference, where I met the CEO of a national chain of extended stay hotels. Out of pure luck, I was sitting at his table in a hotel ballroom while I awaited my speaking slot after a few introductions and awards. When I saw his name tag and the company name, I made him promise me that we could talk after my session. He happily agreed and waited for me in the lobby after the event. The free open bar with top-shelf spirits could have also had an impact on his commitment.

I gave him a very brief overview of the disappearing services that I provide, and he was very intrigued. While displaying genuine interest, I could detect a hint of concern from his face over why I was sharing this information. I told him that I often run into check-in issues at his hotels due to strict identity verification protocols. These places can be stricter than a traditional hotel since guests will often stay weeks or months while working locally in various industries. They always want to know exactly who is staying there and who should not be present on the grounds. They also want to make sure they get reimbursed from the companies that are providing lodging for their employees.

Once he interrupted with, "How can I help?". I knew we would be long-term friends. I told him that there are two things that can help me and numerous clients that find themselves in danger. The first is a fast-track check-in option that requires no identity verification, and the second is the same discount that he applies to his big customers. When a typical traveler shows up to rent a room, he or she may have to pay $160 a night while the fracking employee in town for a few weeks is quoted $55. He was adamant that he would make sure that I get the absolute bulk rates but was not sure how to tackle the identification issue. I did not necessarily need his plan, as I already had my own. I just didn't know if he would agree.

My proposal to him was to add my company as a customer within his online billing system. I had a legitimate LLC that was not tied to my name, but possessed purchasing power and had a reliable funding source. His company would issue me a customer number and allow me to book rooms online through their partner portal for the discount. I could book rooms that would not require payment from the person checking-in, and my company could be billed after checkout. This was all fairly straightforward and would allow me to receive the lowest pricing. The real power in this proposal was that he would add the following within the notes section, visible during the check-in process.

"This reservation was conducted through the office of our headquarters. Mr. (CEO NAME) has personally assured the guest that check-in will be expedited without the need for any verification of identification or payment. The customer is to be billed Net-30."

He agreed and had his office set me up the week following the conference. It was nothing more than a typical commercial account, but that small note made all the difference. Most employees saw it while checking-in my clients and immediately offered a higher level of service

without ID requirements. On one occasion, my client received great aggravation due to the resistance on providing ID. She asked the reception desk to look for a note on the account, and it was smooth sailing from there.

I logged in to my online portal for this extended stay hotel chain and located a hotel an hour outside of our location. I made a reservation for 30 days and received a rate 75% lower than retail price. I was able to secure a room with a full kitchen, two isolated bedrooms, and two bathrooms. It would not be the Ritz, but it would be better than the current accommodations. Jim and his family began packing.

You may wonder why I didn't just start at the extended stay hotel and avoid the temporary stay at the Hampton Inn. The reason is out of respect to my friend that owns the extended stay hotels. I promised him that I would never send a client that would cause any type of issue toward his company or employees. I wanted to make sure we were clean from any followers that would notify the world that "enemy number one" was at a property owned by my friend. Therefore, I never start at one of those locations. That step needs to offer a clean spot that can be used long-term if necessary.

Jim's co-workers safely escorted him and his family in their off-duty vehicles to the new extended stay option. As expected, they were never prompted for any type of payment or identification, and only had to show the printed reservation confirmation and purchase order created by my company to pay the bill afterward. Neither Jim nor his wife checked the family into the hotel. One of his friends took care of everything and spent less than five minutes in the lobby. They now had a place to call home for a while.

I gave Jim a week to tackle his own issues with his employer and the situation he was in. When he reached out to talk about long-term plans, he asked if I would come see him personally. I would have it no other way. When I arrived, he went straight to the point. "I put my house up for sale, my friends moved all of my belongings into storage, and my wife never wants to set foot in that neighborhood again", he explained in a very monotone, factual voice. "What do we do now?" he asked, understanding that walking into a new home was not feasible financially. I asked him if he ever considered being a nomad, which he did not answer. "Hear me out", I requested, and I started to explain the concept of the official nomad in terms of home domicile in the United States. I gave him the following pitch.

"Imagine you are retired, your kids are grown and out of the house, and you are ready to downsize. Maybe you live in a cold area, and the idea of chasing the sun is appealing. You decide that you and your spouse are going to sell all of your belongings, buy an RV, and follow the weather. You hang out in Florida in the winters and explore the national parks in the summer. You live in your RV and do not have a state to really call your own. This scenario occurs to thousands of people every year, and those couples chase their dreams while enjoying

the freedom of the life as a nomad. In fact, there are three states that recognize a defined 'nomad' and provide a home state without any physical residence within the boundaries."

The skepticism started to break a bit, but he still did not understand how this applied to him. I continued my proposal.

"Think about those retirees. They must possess a driver's license and an official mailing address which can be used on any government document. These people still exist and must have an address lined up to receive mail, file taxes, obtain a passport, and maintain credit. Florida, South Dakota, and Texas fill the void for these retirees needing an official home base. The beauty of this option is that being retired or possessing an RV is not required. Anyone can become a nomad, as long as you obey all of the laws surrounding this option."

My ideas were starting to click with him, and the questions began to fly out of Jim such as, "Is it affordable? Can I have a driver's license without my home address on it? Would this buy us some time to figure out the next steps?", and many others. I responded "Yes to all".

Jim was the perfect candidate for nomad conversion. He was in a tough predicament and needed time. It would be months before any investigation was complete. He had nowhere stable to stay. He was not sure what the future held. He did not know if he would need to move out of state or if the day would come where he could return to the town where he worked his entire career. Ultimately, he was in no place to make any type of commitment and needed to float for a bit. I laid out the entire process of becoming a legal nomad and the entire family agreed to cooperate with the plan. The remaining content of this chapter details every step, including my mistakes made along the way.

I had personally become a legal nomad a couple of years prior to this incident. I always make myself the guinea pig for all of my weird ideas, and this one needed to be bulletproof before I offered it within my menu of services. In 2014, I took an early retirement from my law enforcement job as a cyber-crimes detective. I sold my home and accepted a new position that would have me traveling extensively. I would no longer be an Illinois resident, but I would also not be connected to any other state. I would be a bit abandoned. I could have easily kept my Illinois driver's license and used a local PO Box, likely not drawing any skepticism, but it felt odd. I had always used the address of the local police department on any government identification, and that seemed inappropriate after retirement. The last thing I wanted was to ruffle any feathers with my previous employer as I started a new venture. After much research, I settled on becoming a nomad within a nomad-friendly state.

My four goals for Jim were as follows, with the reasons for each included.

Obtain a new physical address. Jim will be selling his home, and he would be legally required to provide his new address to the Department of Motor Vehicles (DMV) upon sale. The moment he supplies the actual place he is staying, it is public information. Most states offer some type of option to purchase various databases. Third-party data mining companies love this, and the state makes a nice profit from our personal details. Within thirty days, the address provided will be available on premium people search websites at less than $15 per query. I can't allow that. Therefore, I need a physical address that can be used on a driver's license, passport application, tax return, or any other legal document. It must also be an address where Jim will never visit. Finally, it must all be legal.

Possess a reliable mail forwarding service. I will be forwarding Jim's postal mail away from his home to a commercial mail receiving agency (CMRA). This will also be public information. Therefore, I need a service that will securely accept all of his mail and send in bundles to any address I specify. This middle-man protects the final destination from public view.

Mislead anyone hunting him or his family. I must purposely pick a physical address that would never be used as an actual residence. I have met privacy seekers that pick random houses and claim they live there. This is irresponsible. I don't want an activist to fire-bomb some innocent person's home thinking they are getting revenge on Jim. His new "home" must be an obvious commercial property that will confuse anyone that spends the resources required to identify the location. He will never set foot anywhere near the location.

Buy as much time as he needed. Finally, I need a solution that will give Jim some breathing room. Becoming a legal nomad can be temporary or permanent. Jim and his family will not need to rush into any long-term commitments and can let this whole situation unfold naturally.

For the sake of this chapter, assume that Jim chose South Dakota. The first step toward establishing residency in a nomad-friendly state is to purchase a Personal Mail Box (PMB), as explained previously. I was able to create an account online in his real name and use a Privacy.com masked debit card to pay for the purchase. Every PMB service I have found possesses awful online security, and I suspect that each have had a data breach of some magnitude. Therefore, I never provide a personal credit card number.

For $300, I obtained a new physical mailing address, mail collection services, forwarding options, and enough postage to easily cover outgoing shipments of mail for the next year. This is a vital first step toward obtaining true privacy with a "ghost address". From this point forward, any time that my client is asked for a physical address by any government or private entity, he will provide this new PMB address. While most PO Box addresses are not allowed on personal documents, such as a loan or driver's license, a PMB is allowed.

Once the PMB was established, it is very important to conduct a test. I sent a letter without a return address to my client at the new PMB address. The package I chose for Jim included a mail scanning feature which emails him an image of the cover of every piece of mail as it arrives. This is a great feature that I enforce with all clients. It is important to know when mail arrives and needs to be addressed. Within a few days, he received notification of the letter, and we were in business. On one occasion, I simply assumed that a PMB was properly created for a client. Due to a bug in the outdated online system, she was given a different box number which did not exist. She missed some important notices from a government agency which caused quite a headache. This was my fault for not testing. Fortunately, a letter to that agency directly from me accepting fault was sufficient to get her back on the right track. I now test all new PMBs.

As stated previously, these PMB services are mostly used by retired couples traveling the world in an RV or pop-up trailer. The privacy policies associated with customer accounts possesses the same security that you would expect from your grandparents. On numerous occasions, I have called the PMB company of my clients, stated I was them, and asked them to read the return addresses of all mail pending in the box. I have never been denied this invasive request. As a test, I once called the service and provided a random PMB number and stated that I was missing an outgoing shipment. The representative quickly provided me the last shipment date and address where it was sent. The security at these places is outright awful. However, I don't have a better solution. Therefore, we will get creative with the shipment address of the bundled mail packages.

Eventually, Jim will buy a new home anonymously and he can open a traditional PO Box a town or two away from his home. He can then have the PMB packages sent to the post office. Until then, he needed to receive his package, and I couldn't take the chance of an adversary calling the PMB company to identify where his shipments were being sent. Therefore, I created a temporary solution.

I contacted an upscale hotel a few miles away from his current extended stay location. I made a one-night reservation in his real name for two weeks from the current date. I secured it with his real credit card and confirmed the cancellation policy. I then requested the PMB to ship all pending mail to my client at the hotel address. Tracking information identified its arrival, and his wife went and picked up the package. She stated that she had an upcoming reservation, but she wanted to pick up a package that recently arrived. The hotel staff verified her identification and retrieved the item from storage. After she had the package in hand, I canceled the pending reservation without any charge on his card. Why did I have to be so sneaky?

If someone convinced the PMB company to disclose the shipment location, this plan did not impact my client's immediate safety. Realistically, no one will ever know any of this happened.

If an adversary identifies the locations of shipped mail a few months later, he or she will waste a lot of time determining if my client is still at the upscale hotel. By then, he will not even be living at the extended stay option twenty minutes away. It is an ideal temporary fix. If I had sent the package to the hotel without making the reservation, it may have been rejected as "Return to Sender". Finally, the PMB is mandated by USPS rules to only ship packages in a confirmed name. Every shipment that Jim requests will have his and his wife's name as the recipient. This needs to be kept in mind at all times, and Jim will need to be selective about delivery.

I must confess that this idea of shipping to random hotels did not come to fruition proactively. It was a reaction to an unpleasant situation of my own. In 2015, I forwarded my PMB mail to an address of a friend whom I would be visiting. The package was delivered to his home in my name before my arrival. I obtained the package during my visit. He had no concerns about privacy and had no objection to me receiving mail at his place. I didn't think anything of this for weeks after my departure. That lack of concern faded away quickly.

My PMB address is publicly available through data brokers such as CLEAR. This is by design. It is an address that can be publicly connected to me without fear of compromising my true location. Someone identified this address and contacted the PMB provider, pretending to be me. The service provided this intruder the last address where a package was sent and a list of pending mail waiting in my box. The subject then attempted to social engineer my friend. He stated that he was with the PMB provider and that a package had been returned undeliverable from my friend's address. The subject then asked my friend where he could send the package so that I could receive it overnight. My friend honestly responded that he did not know my home address, and the attempt failed.

I learned two valuable lessons. First, never forward mail from a PMB that could compromise you. Send it to a UPS store or a hotel. This eliminates a personal attack surface. Next, I learned that your friends and family can be the weakest link. If my friend had fallen for the attack, the intruder may now know where I live. To this day, I have no idea who the person was. I only received an anonymous email soon after my friend told me about the call. The subject confessed to his actions but never disclosed his motivation. OK, back to Jim.

The only negative response to this scenario is the mischievous feeling of accomplishment by Jim's wife. After she received the forwarded package at a hotel where she never stayed, containing out of state vehicle license plates from her "ghost address", she was hooked. I had created a monster. In her mind, she was Jason Bourne, and a bit too excited for the next level. I watched her closely after that. Jim also had the nomad bug when he switched his license plates from the old state to the new. He seemed excited that there was a tangible step in the right direction, and he seemed to have a sense of a future solution to all of his problems. Next, it was time to make them official residents of the State of South Dakota.

The eight-hour road trip was full of excitement. Jim and his wife interrogated me on the next steps and other levels of privacy they could achieve. I shared a bit about my personal strategy and gave them some insight into the next tier. More importantly, the drive gave me time to prepare them for the various roadblocks they would face after this next task. We talked about address change notifications, credit freeze problems, insurance issues, and a slew of other complications they had not yet considered. I assured them that I had solutions for them, but it would not always be easy. Their lives had changed, and they had no option to return to the previous version. There would be many additional hurdles to face.

We arrived at the hotel, where I had arranged two rooms under an alias name. I have not stayed in a hotel under my real name in a decade, so I did not think much of this. Jim and his wife were not prepared. The three of us walked to the counter and I supplied my alias name as a new check-in and waited for the attendant to retrieve the reservation. Jim and his wife simply stared at me with open jaws. I should have told them my plan, as they looked at me like betrayed children. I provided a credit card in the alias name and a rewards card from that hotel chain matching the identity for the reservation. I was not asked for identification, as I had obtained the highest tier of their frequent traveler program. At that level, the rules rarely apply, and the hotel clerk's job is to make the stay as perfect as possible. I had identification available if necessary, but it is rarely required.

My mistake here was not notifying my client of every action. The desk clerk picked up on their looks of surprise at my name, and likely thought I was involved in some illegal activity. I now explain everything at all times, and never present any surprises.

I gave them their room keys and we agreed to meet in the morning for breakfast (free of course, thanks to the rewards status). My friends and family from my home town always seem impressed at the perks I receive when we travel together. The truth is that it is a sad moment when you achieve elite status. It clearly reminds you that you have no social life and that you may be overly dedicated to your work. I would trade in all of my perks in exchange for the lost time due to extensive travels. That is likely the most personal piece you will get from me here.

In the morning, I outlined the plan. I was heavily armed with all of my previous mistakes made in South Dakota, and I anticipated a smooth process. Jim and his wife seemed overly nervous, but I knew the feeling. The day I received my driver's license as a nomad, listing a ghost address as my home, I was beyond thrilled. It was my first experience with the process, and I expected to get arrested. It seemed so shady, but I now know better. I was about to walk two clients through the routine with my head high, confident in my methods and the laws that allowed the process.

There was one hiccup during my own residency process that I will never forget, and which I have never replicated. When I arrived at the DMV to obtain a nomad license, I had no proof that I had stayed the night before in the county of the DMV building. This is a stern requirement that is heavily enforced, likely to make sure the county received the tax revenue from a lodging stay. I had my hotel receipt, but it was in an alias name. I had to leave the DMV, return to the hotel, convince the front desk to print an additional receipt in my real name, and return to the DMV for more scrutiny. I eliminated that alias afterward, as it was now directly associated with my true name within the Hilton system. Another lesson learned.

Before we all left the hotel, I asked the front desk clerk to print two separate receipts for the two rooms. I also asked that she include each of my clients on the independent receipts. I apologized for the trouble in advance and told her, "You know how bosses can be, everything must be perfect". She gave a nod as if she could relate and issued me two receipts. Jim's name was on one and his wife's on the other. We were ready for the show.

The DMV was only a few minutes away from the hotel, and we arrived before the car could properly heat. We sat in the car for a moment and made sure everyone was ready. I told them to follow my lead and assured them that we were about to conduct a very legitimate process. Jim was ready to knock it out, but his wife appeared nervous. We stepped in to an empty DMV building with three employees ready to help. In South Dakota, you are immediately intercepted by a "greeter" who is present to help with the process. There are so many retirees that technically reside in this county, that the bulk of their business is out-of-towners that have no clue what to do. This is very helpful, as it removes the scrutiny on our plans. I opened the dialogue immediately with "Hi Tom, good to see you again!", before the greeter had a chance to speak. He vaguely remembered me but was not sure why. I continued with "I brought Jim and his wife with me to get them set up as nomads since they just bought their first RV, and our first stop is Mount Rushmore!", which lit up Tom's face.

I have found this demeanor to create a great vibe within the office, and Tom likes to tell stories about his own RV adventures. He also happens to be very fond of Mt. Rushmore. This introduction was no accident. Tom works part-time on Mondays and Wednesdays. His work schedule and dedication to the carved presidents is publicly available on his Facebook profile. I have no shame; I will use every resource to my advantage. When Tom is happy, he makes sure that my clients have no issues with their new nomad status.

Tom verified that both Jim and his wife possessed the following documents.

- Current out-of-state driver's license
- Secondary ID (passport or certified birth certificate)
- Verification of SSN (original card or 1099 form)
- Receipts showing lodging in the county within the past year

- Additional documentation of South Dakota address
- South Dakota Residency Affidavit

Most of these items should make sense for any DMV license transfer. The additional documentation of the South Dakota address is not absolutely required but has been very helpful in the past. Showing your PMB company paperwork with your name and new address is usually sufficient. However, I have had two situations where the DMV employee demanded to see something official associating the person in front of her with the address being requested for the license. This is where the vehicle registration comes in. Since I already registered Jim's vehicle in his and his wife's name at his new PMB address, I had official documentation from the state. Showing the title or registration verification has always been sufficient. If a car had not been registered, I could have presented an Amazon invoice or bill as proof. The most important lesson is to have more than you need upon arrival.

Tom confirmed that their proof of a local PMB satisfied the state requirement for residency, and they could legally call South Dakota their home if they wished. He informed them not to worry about the notification of potential jury duty. If they would be selected, a simple call identifying themselves as full-time travelers who do not actually live in the state would remove them from any obligations. Jim and his wife eagerly signed, and they were ushered toward a DMV clerk. After a quick eye test and photograph, they both possessed South Dakota driver's licenses, and they were now officially residents of the state. While I wish I could discuss the fanfare surrounding this event, there was none. We quietly walked out and returned to the car.

"Is that it?" Jim asked. I confirmed that we were done. He and his wife giggled a bit and I saw a bit of hope in his face. He had been beaten hard by the events over the past month, but this was a sign of a silver lining. We drove 8 hours back to his extended stay lodging and had a closing conversation.

I advised him that the big steps had been taken to buy some time while still maintaining his life's responsibilities. He now needed to take the time to change the mailing addresses on file for every bank, utility, insurance, or financial company that he can think of where he may have an account. Basically, he needs to treat this as a move from one house to another. Additionally, he needed to visit a post office and submit an official change of address form, choosing the "permanent" option on the card. This would forward his mail for several months while he identified other accounts to update. As far as any entity is concerned, his new PMB address is his home.

I should pause a moment and reflect on what this really accomplished. On the surface, he simply possesses a new driver's license and vehicle registration. This alone does not physically protect his family from danger. The power of this strategy is the ability to use it as a tool for future protection. Please let me explain.

While Jim is in limbo and awaiting a verdict in reference to the shooting, he will be on the move. He still needs access to his mail. He still needs to use credit cards and pay his bills. He does not want to return to his home. This solution provided a secure repository for the collection and distribution of mail on his own terms. More importantly, he has a physical address to give to companies that apply scrutiny toward changes of address. If he simply acquired a PO Box and provided the new address to his credit card provider, that company would maintain his last known physical address on file. This PMB address replaces all addresses on file and passes USPS verification checks. Jim can use this address for the rest of his life if he chooses.

It is well documented that states sell driver's license data to third-party companies. The address on your license is publicly available within dozens of free and premium search services. When the next person wishing harm on Jim looks to see where he moved, the only data available will be a commercial receiving service where he has never been present. When he sells his home, the title and transaction forms will be public data. He must disclose a current address during the sale. He now has a safe address to provide where a check can be received. When this PMB is announced in the local paper within property transactions, he has no concern. Jim can still exist, but not be found.

Jim was very selective of the details he was willing to share publicly, and his wife was even less revealing. You may be wondering why I referred to her as "his wife" so much, and never provided a real or alias name. This was her choice. She asked to never be named at all, noting a passage in my previous book *Hiding from the Internet*:

"Be careful when you select an alias name to use. Most people choose something they believe to be random but can actually be very revealing. It might be the name of a celebrity that you like or a distant relative that has passed. Either could be used to associate you to your alias or potential online security questions."

She simply asked to only be referred to as Jim's wife at all times. I respect her decision. Jim would later be cleared in this incident and the shooting was ruled as justified. He left law enforcement completely, and he continues to travel extensively with his family as nomads of South Dakota. The threats died off, but they are still always looking over their shoulders. I consider Jim a success. Things could always have been done better, and I learn from every experience. The protections put into place for Jim had unintended benefits later. The following happened several months after Jim became a nomad.

- An unknown individual attempted to place a "mail hold" on Jim's mail. This is common during scam attempts when the suspect does not want the victim to receive any notifications of financial transfers. Since Jim's mail is at a PMB registered with the USPS, a mail stop was not possible.

- This same individual then attempted a permanent change of address in order to forward future mail to another PO Box. Again, this was declined due to the mail being collected at a PMB. The PMB services do not allow permanent forwarding as you would conduct during a move.
- The suspect attempted to open a new retirement account in Jim's name with his DOB and SSN. Jim received a letter from this bank asking him to remove his credit freeze before any new accounts were requested.
- Someone attempted a SIM swapping attack toward Jim's cellular number which was released during a doxing attack after the shooting. Per the instruction previously, Jim ported his known number to Google Voice and adopted a new prepaid account. The SIM attack was unsuccessful.
- Unauthorized people attempted to make changes to Jim's personal checking account during social engineering attempts toward the bank. The attackers could not identify the telephone number for the account when asked. When the bank called a verified number on file, it forwarded to Jim's MySudo app and he took the call, canceling the changes.

If you were targeted in this manner, would you be protected? I hope this provides enough justification for you to start making changes right away.

Chapter Nineteen

My Successes and Failures: Mary Doe

During 2019 and 2020, I witnessed more extortion attempts toward my clients each year than the past decade's cases combined. The ability to mask a true identity on the internet, and the online presence of practically everyone's breached passwords, has created an opportunity for mean people to easily act on their criminal impulses. My online extortion investigations usually fall into one of the following categories.

Stolen Photos: This is the most common scenario. As I write this, I have three pending emails asking for help. Typically, a criminal gains access to online backups of personal photos, usually automated via a mobile device, and identifies any images containing nudity or sexual acts. The suspect then threatens to release the images unless the victim provides either payment or additional nude photos. The summary on the following pages provides more details.

Hidden Cameras: I have represented clients who have been the victim of hidden cameras placed in hotel bathrooms, locker rooms, and other places of potential nudity. The recorded videos are then used for extortion. In one scenario, the victim refused to pay, and the video of her showering was sent to all of her co-workers. In another scenario, a woman seduced my client, brought him back to her hotel, and recorded a sexual encounter. She then threatened release of the video if he did not pay her $100,000. It was a targeted and well executed setup.

Past Mistakes: In 2020, I assisted two clients with issues from their past. In one, a wealthy business man was contacted by a stranger who claimed to possess a VHS video from 1987 depicting him in an "unflattering way" which could have an impact on his reputation with his company. In the other scenario, my client was sent images scanned from old photographs showing him in "blackface" while in college. After refusing to pay $10,000, the images were published online and forwarded to the board members of his company.

Stolen Accounts: Occasionally, I meet a client who has lost access to a popular online account to a hacker. This includes celebrities who possess social network profiles with millions of followers. There is a huge black market for these accounts, as they can be used to send spam or harm the reputation of the account holder.

These types of extortion attempts seem to be getting worse. The following pages present my work with "Mary". She and I hope that the details shared here will help others in similar situations.

I met Mary through a Hollywood acquaintance. She is not a household name, but is a very talented actress with an impressive filmography. She reached out to me and we scheduled a call over Wickr. Over the hour-long conversation, she explained the hell she was going through and I began creating a strategy to gain control of the situation. The following outlines every detail of her encounter.

During a Saturday evening out with friends, she received a SMS text message on her iPhone from a strange number. It simply stated "I have your nudes, want proof?". Before she could respond, the suspect began sending images of her to her phone. These included intimate photos she had taken and previously sent to her boyfriend. She responded with "Who is this?" and the suspect began making demands. He threatened to publish the photos to the internet and send copies to all of her friends and family if she did not pay him $50,000 in Bitcoin. He advised she had 24 hours. An hour after these messages, she had contacted me for advice.

My first suggestion was to cease all communication and ignore any further messages. In general, I always recommend this. The moment you respond to extortion, the offender knows you have seen the messages and almost always becomes more aggressive. Preferably, no one should ever respond to these. There is usually nothing you can do or say to prevent publication of the images. We were past that, so it was time to begin the investigation.

The telephone number of the suspect displayed a Los Angeles area code, but that alone means nothing. I queried the number through dozens of online search tools which only revealed "Los Angeles, CA" as the subscriber information. This confirmed my suspicion that this was a VOIP number which was not assigned to a cellular account. I logged in to a free trial account at Twilio, opened the dashboard, clicked "Lookup", selected the "name" and "carrier" options, and conducted a search. The result identified the VOIP provider as "go-text.me". This site, located at https://go-text.me, confirms the number to be associated with a mobile app which allows "Unlimited texts and calls to the US & Canada from your own real phone number". These numbers are commonly used to harass victims without disclosing a true identity. I now knew the service, but had no details to identify the suspect.

Next, I wanted to determine the way that the suspect accessed her photos. I confirmed that she synchronized all of her iPhone content to iCloud, including photos. I had her log in to her Apple account through a web browser and click on the Devices option. This displayed only her iPhone and MacBook laptop. This eliminated the possibility of another device associated with her account. However, it does not disclose access to her iCloud via web browser. While logged in to her iCloud account, I had her click on the "Sign out of all browsers" option and change her password to something randomly generated by a password manager. Next, I had her conduct a search within the email account associated with her Apple ID for "Apple ID was used to sign in". This revealed a message in her spam folder announcing that someone had successfully accessed her iCloud account which included the date, time, time zone of the

user, and browser details. She confirmed that she has never accessed her account from a browser.

I now knew that someone had accessed her account at a specific time, and could make assumptions about the activity within her account. He likely already downloaded all of her photos, contacts, email, and other details. A quick search of her email address within my own data breach collection identified two commonly used passwords. She confirmed that one of them was her previous Apple ID password. I now assumed that the suspect found her email address online, identified a known password within a public breach, accessed her iCloud account using those details, identified her telephone number via her Apple account, downloaded all of her content, and then began the extortion attempt.

The suspect continued threatening her via text message and became more aggressive as she ignored the communication. She seemed willing to pay money to the hacker, but I always discourage that. I have hesitantly assisted ransom payments for clients, but the outcome was always the same. Even after the suspect received payment, he or she went ahead and published the content. There is no honor among thieves. I explained that there was a very good chance that these images would be published online regardless of meeting any demands, and there was little to nothing she could do at this time. If she paid the extortion, the attacker would keep the images and probably post them later. It would also make her a bigger target. If she paid once, she would likely pay again. Paying into ransom and extortion demands is never a solution, it is usually the beginning of a bigger problem.

The next morning, she woke to find a slew of text messages from the suspect. Although her 24 hours had not expired, he began posting content to the internet. This confirmed my assumption that he would publish content regardless of payment. One of the messages contained a link to a page on Pornhub.com. The page presented a video which cycled through her stolen sensitive images. Her name was present within the title of the video, similar to "Mary Doe naked and exposed". She was devastated to say the least. His text messages indicated that he had not sent this link to anyone yet, but demanded immediate payment in order to keep it private. He sent her a list of all contacts from her phone, which had been previously synchronized to her iCloud account. He informed her that she had two hours to send the Bitcoin or else all of these contacts would receive this link.

Mary and I discussed the options. She said that she could raise the $50,000, but it would take some time and would cause financial strain. I again informed her that paying the ransom would not eliminate the potential of public exposure. The premature posting of images and childish language convinced me this was an immature young adult who simply knew enough about internet security to be dangerous. I discouraged any payment and convinced her to focus on damage control.

During our conversation, the suspect began sending the link to various members of her immediate family. Again, he was dishonoring his own deadline for payment. He sent the messages to the email addresses of her mother and brothers from a ProtonMail address in her name, similar to therealmarydoe@protonmail.com. The messages included the text of "Hey, check out my new promo pics for my next movie!" and a link to the pornographic images. While Mary began contacting her family in order to warn them about the abuse, I focused on removing the content from Pornhub.

Fortunately, removing content from porn sites is extremely easy. Most of them immediately remove the requested URLs and perform a manual review afterward. I submitted a request through the Pornhub removal page and cited the following reasons.

"Revenge porn, blackmail, & intimidation through a video published without authorization."

Almost immediately after the submission, the Pornhub link began forwarding to an error page. The content was no longer available, for now. I know from experience that this suspect was not likely to go away, and he would probably become more aggressive. However, the messages currently waiting in people's inboxes would not expose my client. We did not respond at all to his messages, and waited for his next move, which came about an hour after his previous contact. He sent Mary a new link to an online blog hosted on a free WordPress profile. This page contained three of the pornographic images of Mary, but the pictures were somewhat sanitized with small black bars covering vital areas to prevent them from technically portraying pornography. I had never seen this modification step before.

I immediately submitted a removal request to the appropriate page on the WordPress platform. I cited the Digital Millennium Copyright Act (DMCA) since Mary owned these images and WordPress may not deem them to be pornography. Within an hour, I received the following response from WordPress.

"We have reviewed your DMCA notice and the material you claim to be infringing. However, because we believe this to be fair use of the material, we will not be removing it at this time. Please note that Section 107 of the copyright law identifies various purposes for which the reproduction of a particular work may be considered fair, such as criticism, comment, news reporting, teaching, scholarship, and research. You are required to give consideration to whether a use of material is fair before submitting a takedown notification, as a result of the decision in Lenz v. Universal. Please note that you may be liable for damages if you "knowingly materially misrepresent" your copyrights – and we may seek to collect those damages."

Not only did WordPress refuse to remove this inappropriate content, they threatened to seek financial damages from me for submitting a removal request, as I briefly explained within a previous chapter. I was shocked and quite angry. I submitted a second submission, but avoided

the DMCA process. Instead, I navigated to the abuse reporting site at https://wordpress.com/abuse. I chose the option of "This content contains my private information" and provided the URL of the exposure. WordPress notified me that the company does not believe "Photos of people", "Publicly available physical addresses, email addresses, or phone numbers", or "Names" to be private information. In the box designated for further information, I entered the following.

"Nude photos on this page depict a person (me) who was a minor. Child pornography is defined as nude photos of a person under the age of eighteen. Please remove these illegal images immediately."

Hold your hate mail. First, my client is an adult in her 20's. The nude images depicted what appears to be a young woman in her late teens or early twenties. Second, I found it unacceptable that WordPress would defend this type of extortion behavior. Finally, I said nothing untrue. The page does contain nude photos. My client was a minor at one time, just not now. Child pornography is illegal. These images are illegal as they were stolen as part of an online intrusion and extortion attempt. Notice I did not state that the images posted were child pornography. Within an hour after submission, the page was removed. You may disagree with my strategy, and I do not recommend that you replicate any of this without legal counsel, but the ultimate goal was reached. The inappropriate content being abused was removed.

The suspect was irate. He did not know with certainty that we had removed the page, but he knew it was gone. His response to our cat-and-mouse game took things to another level. He purchased a domain name and hosting account in order to continue publication of the nude photos. He then forwarded the new web page address to the same contacts as the previous attempts.

This presents the most difficult type of content to remove. Since this is a personal website, I cannot submit a request to the host, such as Pornhub or WordPress. Obviously, a removal request to the suspect would be pointless. The suspect had enabled privacy protection which hides the identity of the owner, which was likely false information anyway. A query of the domain, which was similar to marydoeexposed.com, identified the web host, which offered the first month of service for less than $1.00. From the host's website, I identified the appropriate abuse contacts. I sent the following email to the abuse team.

"The website located at marydoeexposed.com contains nude images of me which were stolen from my iCloud account. Distribution of these images through your servers is a violation of copyright laws and subject to civil litigation. I demand that these images are removed immediately."

The entire account was suspended within hours. Mary and I both knew that this game could go on forever. We agreed it was time to step up the investigation into the identity of the suspect. Mary filed a police report with her local police department while I began digging. While I have witnessed some law enforcement agencies take immediate action, the reality is that their resources are limited. If a local department does not possess officers trained in cyber investigations, they simply do not have the tools or knowledge required to tackle these sensitive investigations. Most departments refer victims to the FBI, which has its own complications. It can take weeks or months for a federal investigation to be approved and launched. While I am happy to cooperate with any law enforcement willing to assist, my priority is to remove content for my client in order to minimize exposure as quickly as possible. Filing the report was only a formality. It notified law enforcement of the incident and allowed them an opportunity to investigate. When I am criticized later during an investigation, which happens often, I can prove that I made an attempt to bring law enforcement into the case. However, I do not wait for them.

I began reviewing all of the online evidence I had captured before removal. This included screen captures of all pages and content. The Pornhub username for the original publication was similar to "ihackcelebs4fun". I began researching this username which mostly forwarded to other Pornhub pages identifying previous victims. However, I located several posts on Reddit from a person with the same moniker. The post matched the activity of posting stolen photos. I decided it was time to initiate contact. I located a Pornhub video which the suspect had posted a month prior to my client's content. I sent a direct message from a covert Reddit account to the suspect's Reddit username and referenced the older video, which was still online. I told him that I had a ton of similar images and asked if he was up for a trade. I offered to send content first so that he knew I was not trying to rip him off. This message was sent at noon on a Sunday, and I had heard nothing back by the end of the day. I assumed this was a dormant account and my message would go ignored.

While I was doing this on Reddit, Mary sent a response via text message to the suspect. She stated that she was working on getting money into Bitcoin, but assured that she had the funding. She insisted that he post no further images, and that she would refuse to send the funds if he did. He agreed to wait until the following day, which bought us some time. There was no intent to send any money. This was simply a ruse to stop the posting game and allow me to focus on the investigation.

At my direction, Mary sent a text message stating, "I tried to pay BTC to the address you gave me but it said bad address. I don't know what to do". The suspect became frustrated, but this is common in extortion. Telling people who are unfamiliar with Bitcoin to send large sums of digital currency is almost always met with problems. He asked which company she used, and she stated, "Coinbase", which is a popular Bitcoin exchange. He asked her about the error message and she played dumb. He then gave her a command for which I was waiting. He

texted, "Send me a screen capture of the error". This excited me because he was opening an opportunity for me to send some bait. I advise Mary to respond, "It says file to large. What is your email? I can send it there".

I was not expecting him to share a personal email account in his real name, but communicating over email can have great advantages. My goal was to send him an image which included embedded tracking software which would disclose his IP address, computer details, and possibly approximate location. Once he disclosed his covert ProtonMail address, I took over all communication. I sent an email from an account through Gmail which I had created in Mary's name. It included a link to an image which I knew would appear as a Photo-shopped file depicting a Coinbase account with a $50,000 balance. The content was not important, but I hoped it would get him excited. Instead, I was counting on him clicking the link without much investigation.

The link was generated by a service called **Canary Tokens** (canarytokens.org). It allows me to send a URL displaying any image desired. When a target clicks the link of the image and views the content, a small script attempts to gather the information about his computer and connection as mentioned previously. This is always a gamble. Tech-savvy people know to look for this and will likely block the attempt. After analyzing all of his communication, he seemed like an anxious person just looking for a quick payday. Within a few moments after sending the link, I received a notification from Canary Tokens that the bait was taken.

The report stated that the offender was on an iPhone and disclosed the IP address of the connection. I had hoped that sending an email instead of text message would encourage him to check from his laptop, but this failed. After a quick search, I determined that the IP address was assigned to a VPN company, and was practically useless. This was also a failure. We were getting closer to him, but were far away from discovering an identity. The suspect responded via text telling Mary to try the payment again. Mary said that she will keep trying if he promised to stop uploading content. He agreed and we closed our investigation for the day. Mary ended the conversation with, "I can get this done first thing tomorrow".

I woke up Monday morning to find an alert of a pending message within my covert Reddit account. The message, from the same username as the suspect Pornhub account, confirmed he would be interested in trading stolen photos. The previous attempt to obtain his IP address through a trap embedded into an image failed, but I found no harm in trying again. This was a different platform and a new day. I created a new infected image and sent it to his Reddit username. I sent a poor quality still capture from a publicly available pornographic video. This was a grey area, as I did not own the image or have authority to distribute it. However, I feel the intent justified the risk. Within seconds, I received a response within the Canary Tokens website. This time, the IP address was not associated with a VPN and the link was not opened

from a mobile device. Instead, the IP address was assigned to a national chain of banks and the computer used was a Windows 10 desktop with the Chrome browser.

I did not want to get my hopes up. While my suspect could be an employee of this bank, he could also be someone using public Wi-Fi at the business, a criminal connecting through a compromised on-site computer, or any other type of proxied association. My research into this bank indicated there were numerous buildings within the metropolitan area of the IP address block. This was a lead too big to ignore, but it would not be easy to isolate a specific offender.

I set my sights on the possibility that my suspect was a bank employee. Banks typically do not offer free Wi-Fi due to security reasons. Checking a Reddit message through a compromised business computer seemed to be a stretch. My hopes were that my offender was just sloppy. I identified the Chief Security Officer for this national chain of banks and contacted his office via telephone. After a few hops, I was connected to his secretary. I calmly and politely explained the situation without providing too many details, and made it very clear that an employee of this bank was using corporate assets during work hours to commit extortion. She seemed to take things seriously and promised to have someone contact me soon. An hour later, I received a call from an attorney representing the bank.

The call was awkward to say the least. It was obvious that the attorney did not want to implicate the bank in any way or acknowledge an internal issue. At one point, he asked, "What are you asking us to do?", which I eagerly answered. I clearly explained that my only goal was to protect my famous client. I had no desire to smear the name of the bank or go public with this information. If the bank was willing to cooperate in identifying the employee responsible for this situation, I was willing to keep it quiet. If the bank refused to cooperate, I was willing to take my evidence to the local police, which would make the entire scandal public information. I expressed my opinion that we both had much to gain by keeping this investigation as quiet as possible.

The attorney quickly ended the call and refused any further contact attempts from me. Lesson learned. Much like my job is to protect my client, corporations only look out for their own best interests. This was a failure. Fortunately, I did not disclose any details which would help them identify the suspect and compromise our own investigation. I went back to the drawing board.

While I was contacting the bank, Mary was receiving additional messages from the suspect. He told her that time was up and either she must pay or he would publish all of her photos directly to her contacts and send copies to various tabloids. He further threatened to create a torrent file which could be seeded in a way which could never be removed. It seemed that we

had stretched his patience. I had yet to hear back from any law enforcement personnel about the possibility of opening an investigation.

I revisited his online presence. I read through every post he had made on Reddit. In retrospect, I should have started there before trying to get his IP address. His post history seemed redacted. There were posts which had been deleted and some which appeared to have modified text. I replicated my search of his posts on a third-party archive called **Pushshift** (pushshift.io). I generated a custom URL which would display all posts made by him as they were archived soon after publication. The exact URL for this example username appeared as follows.

api.pushshift.io/reddit/search/comment/?author=ihackcelebs4fun&sort=asc&size=1000

The result was over 200 posts made by the suspect over the past two years. This presented much more content than I found on his live profile. I began devouring posts for any further clues. Within this treasure, I found posts about banking, which fit the employment at the bank identified in the IP address. I also found numerous posts within the Pomona, California Subreddit (https://reddit.com/r/Pomona), which was within the geographical area of the IP address. I was getting closer. The gold prize was the following deleted message.

2019 Acura TLX Tech Trim in like-new condition. 3457 miles. No damage.

https://imgur.com/a/XaOj4rC

The Imgur link displayed several photos of a vehicle, and the post was recent (2019). None of the images displayed a license plate, but this was my next solid lead. I replicated the search of "2019 Acura TLX Tech Trim" on Craigslist and received the following post.

2019 Acura TLX Tech Trim in like-new condition. 3457 miles. No damage. Call Matt at (909) [REDACTED].

The post included the full telephone number and the same photos as linked from the Reddit post. I now knew his name was potentially Matt, he might work at a specific bank in the area of Pomona, California, and he might own a 2019 Acura. I replicated my search on Twilio of this number which provided a potential last name. I searched this name on LinkedIn, but received no results. I eventually found a person with this name from Pomona on Twitter. However, there was no direct connection from that account to my suspect. I presented all of my information to Mary, and proposed one last desperate attempt.

Since time was not on our side, and we expected the suspect to blast her details to all of her personal and work contacts, I proposed we call him out. Tell him what we "know" about him

and hope it is right. If we are wrong, it may make him laugh and go crazy online. If we are right, it may scare him. In my mind, we had nothing to lose. I was confident the suspect planned on publishing her photos regardless of payment. She agreed with my plan, and I sent the following email to the ProtonMail address received earlier. I placed [REDACTED] in place of the actual details which I disclosed to him.

"Hi Matt,

I am assisting Mary Doe with the investigation into your extortion attempts. My final report has identified you as Matt [REDACTED]. You work at the [REDACTED] branch of [REDACTED] Bank. You drive a 2019 Acura which you are having trouble selling. I have evidence that you have used computers owned by your employer as part of this crime. Since these are bank assets associated with a corporation covered under FDIC rules and laws, there are substantial federal offenses for which you can be charged. Mary and I are still determining our next actions. For now, we are demanding you to cease all distribution of content while destroying all related data. In return, we will consider keeping our evidence to ourselves. If we receive no response from you, we will forward this content to your supervisor, [REDACTED], as well as Detective [REDACTED] at the Pomona Police Department. Extortion sucks, eh? You can respond here or contact me directly at [REDACTED]."

This is where I want to tell you that he was scared. I want to close this chapter with a victory and messages from the suspect pleading with us to show mercy toward him. That would be untrue. He did not respond to me at all. Instead, he released all of the images as promised and sent links via email to every contact on my client's phone. Mary was officially exposed to the world.

You may believe I reacted foolishly. You are right. It was a desperate attempt, and it failed. It expedited us into the position in which we would have likely found ourselves, even if we had cooperated and given money. I began removing the online content he published, which was fairly successful. He simply replicated his methods of publication from earlier, and I reactively tackled each exposure. He never posted a torrent file, but the damage was heavy. Numerous friends, family members, associates, co-workers, and business interests of Mary viewed the sensitive photos. All of them will say this event had no impact on their relationship with Mary, but I don't believe that. Today, all of the content has been removed.

A few days after the final exposure, a detective from Mary's local police department announced she would be opening an investigation. I made full disclosure of my actions, and accepted all responsibility for the outcome. I was chastised for a few minutes, but we then began strategizing about the next steps. The detective was very sharp, but had no experience with computer crimes. However, she had something more powerful. The detective could request court orders.

She first targeted Pornhub for information about the uploader, but they are a Canadian company. Her U.S. court orders would be of little help. She then reached out to a liaison with the Royal Canadian Mounted Police (RCMP), and they agreed to create a Canadian order on her behalf. This is actually quite common in law enforcement. While she waited, she issued a court order to Reddit demanding information on the account I had located. Reddit confirmed the user's IP addresses and Gmail address provided during creation. A court order to Google provided enough information to confirm the identity of the suspect. A warrant was issued and he was arrested within a week.

I am intentionally leaving out some of the details at the request of the detective who worked the case. However, I can disclose where I was wrong. My fatal mistake was assuming the vehicle posted on Reddit belonged to my suspect. It did not. In fact, we have no idea why he posted those images. Getting this wrong led me to disclose a name to the suspect of which he had likely never known. My education from this is that any suspect can really throw off an investigator by posting a vehicle for sale which has no connection to him.

The suspect did work for the bank, but not at any local branch. Enough of my email was wrong that he felt confident releasing all of the photos. A search warrant for his laptop, which had been seized during his arrest, indicated that this was the seventh incident of attempted extortion. Five, including my client, never paid. Two paid the full amount requested. All seven victims had their photos released publicly. Because of this, I don't have regret in my actions. It was a lose-lose situation. However, I now handle these extremely differently.

I tell all of my clients, regardless of the situation, absolutely cease all communication with the suspect. There is nothing to gain. Furthermore, no response to the extortion at all has been the most successful strategy I have found. If you ever receive an extortion attempt, I encourage you to completely ignore the demands. Paying the ransom usually results in published data anyway. Responses confirm that the suspect has your attention. Notify law enforcement, and hope that your local agency has the resources to investigate.

After this event, Mary obtained all new hardware, online accounts, mobile plans, and alias profiles as explained throughout this book. The Apple account was completely deleted. The suspect was charged with several counts of extortion, released after posting bail, and is awaiting trial during the writing of this chapter. Neither Mary nor I have seen or spoken to him and he has made no attempt to contact either of us. I watch the case closely, and I will be present when Mary testifies.

I want to close this chapter with some lessons learned which may help readers digest the recommendations presented toward the beginning of the book. My focus here is to simply present the methods which could have prevented the entire mess. Please know that I am not blaming Mary. I have executed very similar digital blunders toward my own profiles before I

jumped into the privacy and security game. Ten years from now, I might be disgusted with my current strategies presented here. Hindsight is always 20/20. Treat all mistakes as an education.

- Mary's Apple account was in her real name and associated with a mobile device serviced in her name. Ideally, Apple (or Google) should never know your true identity. This way, social engineering attacks toward Apple are very difficult. If a suspect does not know the name you used to create an account, abuse of telephone, email, and in-store support should be quite difficult.
- Mary's email address to access her Apple account was a publicly identifiable personal address. Most of us have at least one email address which is publicly associated to our name through online people search sites, data breaches, or social networks. The email address connected to an Apple ID or Google account should always be a unique dedicated generic address. It should not be used anywhere else. This prevents attempted password resets and login attempts.
- Mary recycled a password from another online service to her Apple account. I have done this before, but I was lucky to avoid any compromised accounts. Every password should be unique for each service. Password managers can generate random options and store them for easy usage.
- Mary's iPhone was configured to enable iCloud synchronization, which is the default option. This copied her contacts, photos, videos, documents, and other details onto Apple's servers. Once the suspect accessed her account, he had his own copy of her data. I insist that any mobile Apple device is never allowed to access iCloud. I also check the online iCloud account associated with an Apple ID on occasion in order to verify that no data is present.
- Mary allowed her mobile device to be the primary storage of personal photos and contacts. Even if she had disabled iCloud, it could have been re-enabled after a major software update. Because of this, we should never store contacts in the default device address book, nor photos on the device's internal storage. Instead, store all contact details within ProtonMail and copy and paste from there when needed. Photos and videos should be occasionally moved to secure storage within a VeraCrypt container and removed from the mobile device.
- The telephone number associated with the Apple ID was Mary's true cellular account. This allowed the suspect to initiate conversation through her native messaging application. If he had attempted a SIM swap or malware attack, he could have had success. If Mary had provided Apple a VOIP number, any attempted attacks would have been minimized. Avoid giving Apple ID (or Google) accounts any number when possible by signing up through their website (instead of from the device). Apple still knows the cell number assigned to the device, but it would not be visible to the suspect within the iCloud account.

Today, Mary has exceptional digital operational security. Occasionally, she forwards ideas which I had never considered. The entire LineageOS section within Chapter Sixteen contains heavy input from her, as she has completely moved on from Apple devices.

Failures

There are plenty more failures that could fill twice the pages currently in this book, such as the following, which all happened to me over the past four years.

I worked with a CEO dealing with death threats, staying at a hotel under an alias, but attending a convention next door under his real name. It did not take long for his adversary to find him and his room using the methods discussed previously. Surprisingly, the suspect did not confront my client, but his restaurant bills were enormous thanks to the culprit's taste for expensive steaks (all billed to my client's room). The intruder creepily stalked my client from a short distance, and I had no clue. At one point he introduced himself to the client's daughter at the hotel pool. I learned about this after the event. This was the last time I tried to run counter-surveillance for a client. I now hire professionals to do the job right.

I assisted a victim of extreme physical abuse received from her husband. She was hospitalized due to his violence. Her mother hired me to remove her from the hospital and take her somewhere safe and away from him. The husband was always by her side to make sure she did not talk with the police. When I saw an opening, I executed my version of an extraction. I tried exiting with the victim in a hospital gown through a fire escape, and hospital security detained me until the police arrived. The police questioned me for over an hour. Not my best execution.

Another domestic violence victim contacted me desperate for assistance leaving her abusive situation. She had no money, and a relocation would not be cheap. I was working with a celebrity at the time on a completely unrelated matter and spoke generically about the situation she was in. He insisted on paying her costs and she was safely relocated under a new alias using the techniques discussed here. She insisted on meeting him to thank him. He wanted to meet her as well. With both clients' consent, I arranged a secure communications channel which either of them could destroy if desired. They hit it off. Too well. She was photographed having lunch with him in Los Angeles, and the photo was published in a tabloid. My job was to create a private world for the client, not place her photo in a magazine. This was a valuable education.

In early 2019, one of my clients received a text message with an attached photo. It was a selfie from her former lover displaying luggage and an airline ticket to the airport near her "anonymous" home. She had been hiding from him after suffering years of physical abuse. Somehow, he had discovered the city she was in, and he appeared determined to come find

her. I needed to buy some time, so I turned the tables on him. I could see the airline carrier from the ticket and the departure and arrival details. Out of desperation, I began sending him text messages stating that his flight had a three-hour delay. He bought it and stayed at home while continuing to send her text messages. He arrived at the airport an hour after his flight had left and discovered there was no delay and that he had missed his flight. I still receive hate mail from him weekly as he has now become my stalker after the client bragged to him about my services (Hi Jerry).

I have been on the receiving end of a felony stop after a stalking suspect called the police and reported me as a kidnapper. I was once declined nomad enrollment on behalf of a client on a late Friday afternoon due to missing paperwork, requiring us both to stay in town until Monday. Once, while impersonating a client during an email attempt to remove online information, I was asked "Is this Michael Bazzell?" by the customer support for the service. While these situations were all quite embarrassing, they were also educational. I will never forget the mistakes I made which led to these failures, and I will never repeat them.

I have also made mistakes in reference to my own privacy strategies. Years ago, I initiated a contract for a new personal home and provided earnest money to the title company from a trust. After everything was accepted and both parties agreed to all contingencies, I had to back out. While visiting the home on several occasions, I realized I had my work phone with me, actively connecting to cell towers. I slipped and took a business call in front of the listing agent. She heard enough of the conversation to know my unique business details. Worse, I made an initial call to the power company from a VOIP number associated with my real name, which was likely added to the profile for this address. It is very possible none of this would have compromised my privacy publicly. I couldn't take that chance. I likely overreacted out of paranoia fueled by my past. The lost earnest money was the expense for that education. I was ready to do it right the next time.

I disclose all of this to stress one important final thought. Achieving extreme privacy is an art. Books full of tutorials such as this lay a good foundation for achieving a level of privacy appropriate for your situation. However, no book will provide everything you need to live a completely invisible life or create a new life for others. My best education has been through experiences and failures. My failure rate at various tasks was very high early in this game. I have been denied utilities in an alias name on behalf of clients more than I have been granted anonymous accounts. I happily admit that I have failed more than I have succeeded, but that ratio becomes lower every year which goes by. In the past year, I have had a 100% success rate with achieving anonymous homes for clients. It took time to develop the proper execution of each technique. Experience will go further for you than any written text. I hope something in this book helps you achieve your privacy goals.

CONCLUSION

There are many other less-than-ideal scenarios which I can never disclose publicly. I will only say that I am honored to have been trusted by so many clients over the past several years. This has created friendships with amazing people, all of which are bonded by the secrets which we have all sworn to keep private. Because of these promises, I have reached the end of the details authorized for publication by my clients. I sincerely thank all of them who allowed me to provide an insight into the need for privacy and security.

Conclusion

I truly hope you never need the strategies discussed here. The best-case scenario is that you had an interesting read about the lengths some people go through to protect their privacy. As stated in the beginning, there will be no time to fix things if something bad happens. Extreme privacy is not reactive. It only works when you proactively protect every level of your own exposure. This requires a lot of effort. However, once everything is in place, you can experience the comfort of knowing you possess a private home for you and your family, secure digital habits, and the knowledge to create a private bubble whenever needed. If any negative incidents come your way, you have a safe retreat which no one knows about. Journalists, private investigators, enemies, and criminals will have no way of finding you. Stay safe, and stay private.

If you have adopted the strategies within this book, congratulations. You are sitting in your anonymous home with no affiliation to your name. The car in your garage possesses license plates that cannot publicly be tracked back to you. You have a ghost address, and appear to be a normal person on paper. You have never been to your "official" address on file. You have trusts and LLCs executed and ready to be used for privacy protection. You possess anonymous payment sources and can tackle daily purchases without exposing yourself. Your email accounts are private and secure, and everything in your digital life possesses unique and randomly generated passwords. You have an extremely hardened life, and will be a very difficult target if anyone should come after you. You are practically invisible.

If you would like to stay updated in reference to the latest privacy, digital security, and online investigation strategies which I teach, please visit **https://inteltechniques.com**. On this site, you can access my weekly podcast, blog, and contact information for live events and personal consultations. Thank you for reading. I wish you the best in your privacy adventure.

MB

Alias Wallets, 261
Amazon, 276
Android Mobile Devices, 40, 505
Apple Computers, 49
Appliance Purchases, 280
Birth Considerations, 364
Blogs, 452
Business Registration, 341
Camera Blocking, 41
CCPA, 438
Census, 440
Certification of Trust, 138
Checking Accounts, 254
CMRA, 11
Contact Information, 412
Covid-19, 463
Credit Fraud Alerts, 460
Credit Freeze, 454
Credit Report, 454
Criminal Info Leakage, 450
Data Archiving, 97
Data Backup, 71
Death Considerations, 366
Device Backup, 28
Disinformation, 396
  Address, 399
  Business, 406
  Death, 408
  Name, 397
  Telephone, 404
DNA Kits, 392
DNS Settings, 82
Doxing, 411
Dual Citizenship, 374
Email Forwarding, 87
Email Usage, 86
Employment, 333
  Contractors, 345
  Self-Employment, 340
  Traditional, 333
Encrypted Calendars, 95
Encrypted Contacts, 95
Encrypted Storage, 71
Family Vulnerabilities, 395
Faraday Bags, 31
Final Arrangements, 367
Financial Data, 394
Financial Leakage, 442
Firearms, 475
Fitness Trackers, 393
Ghost Addresses, 11
Hidden Cameras, 216
Home Firewall, 295
Home Privacy, 467
Home Purchase, 221
  Nomad, 242
Home Sale, 243
Home Security, 469
Hotels, 205
ID Scanning and Copying, 262
Insurance, 116, 191, 264
Internet of Things, 387
Internet Service, 271
IRS Registration, 343
Kindles, 390
Legal Infrastructure, 119
Libelous, 446
License Plate Readers, 196, 239
LLCs, 143, 158
LineageOS, 505
Linux Computers, 60, 479
Linux Mobile Devices, 41
Living Trusts, 120
Mail Forwarding, 13
Marriage Considerations, 362
Medical Services, 283
Microphone Blocking, 41
Mobile Devices, 17
  Firewall, 44
  Tracking, 463
Monitoring, 410
Moving Services, 278
MySudo, 25
Name Changes, 360
Neighbors, 237
Nomad Residency Affidavit, 110
Nomad Residency, 105
Number Forwarding, 37
Number Porting, 34
Online Content Removal, 441
OnlyKey, 492
Pagers, 45
Password Managers, 64
Payment Processing, 344
Payments, 245
Personal Data Removal, 413
Personal Mail Box (PMB), 12
Pets, 349
Photo Leakage, 441
Physical Privacy, 467
PO Box, 11
Prepaid Credit Cards, 247
Privacy.com, 250
Proactive Online Content, 452
Purchase Considerations, 287
Rental Homes, 214
Reputation Information Leakage, 443
Right to be Forgotten, 451
Routers, 321
  Portable, 321
  Wireless, 318
Schooling from Home, 465
Secondary Credit Cards, 255
Secondary Devices, 29
Secure Messaging, 24
Secured Credit Cards, 260
Telephone Usage, 19, 32
Tor Browser, 103
Traveling, 98
Trust Amendments, 135
Trustees, 141
Trusts, 128
Two Factor Authentication, 69, 489
USB Operating Systems, 487
Utilities, 269
Vehicles, 163
  Options, 192
  Privacy, 197
  Purchase, 175
  Retitling, 164
  Services, 193
  Tracking, 199
Virtual Currencies, 289, 345
Virtual Machines, 478
Virtual Private Network, 26, 83, 301
Voice Over IP, 495
Web Browsers, 74
Will, 368
  Living, 368
  Traditional, 370
Windows Computers, 56
Working from Home, 465

Made in the USA
Columbia, SC
29 May 2020

"MY SUCCESSES AND FAILURES WHILE MAKING PEOPLE DISAPPEAR"

Michael Bazzell has helped hundreds of celebrities, billionaires, and everyday citizens disappear completely from public view. He is now known in Hollywood as the guy that "fixes" things. His previous books about privacy were mostly REACTIVE and he focused on ways to hide information, clean up an online presence, and sanitize public records to avoid unwanted exposure. This 565-page book is PROACTIVE. It is about starting over. It is the complete guide that he would give to any new client in an extreme situation. It leaves nothing out, and provides explicit details of every step he takes to make someone completely disappear, including document templates and a chronological order of events. The information shared in this book is based on real experiences with his actual clients, and is unlike any content ever released in his other books. The stories are all true, with the exception of changed names, locations, and minor details in order to protect the privacy of those described.

About the Author: Michael Bazzell investigated computer crimes on behalf of the government for over 20 years. During the majority of that time, he was assigned to the FBI's Cyber Crimes Task Force where he focused on various online investigations and new open source intelligence (OSINT) collection techniques. He has trained thousands of individuals in the use of his investigative methods and privacy control strategies. After leaving government work, he served as the technical advisor for the first season of the television hacker drama *Mr. Robot*. His books *Open Source Intelligence Techniques* and *Extreme Privacy* are used by several government agencies as training manuals for intelligence gathering and privacy hardening. He now hosts the weekly *Privacy, Security, and OSINT Show*, and assists individual clients in achieving ultimate privacy, both proactively and as a response to an undesired situation.

INTELTECHNIQUES.COM

ISBN 9798643343707

P9-ANI-899